ÜBER DIE TEILER DER NULL UND DIE ZERLEGUNG VON RINGEN

INAUGURAL-DISSERTATION

ZUR

ERLANGUNG DER DOKTORWÜRDE DER HOHEN PHILOSOPHISCHEN FAKULTÄT DER UNIVERSITÄT MARBURG

VORGELEGT VON

ADOLF FRAENKEL
AUS MÜNCHEN

MARBURG 1914

ÜBER DIE TEILER DER NULL UND DIE ZERLEGUNG VON RINGEN

INAUGURAL-DISSERTATION

ZUR

ERLANGUNG DER DOKTORWÜRDE DER HOHEN PHILOSOPHISCHEN FAKULTÄT DER UNIVERSITÄT MARBURG

ACAD.
LUGD.BAT.
BIBL.

VORGELEGT VON

ADOLF FRAENKEL
AUS MÜNCHEN

MARBURG 1914

Von der Philosophischen Fakultät als Dissertation angenommen am 20. Januar 1914.

Berichterstatter: Herr Geh. Regierungsrat Professor Dr. K. Hensel.

Sonderabdruck aus dem Journal für die
reine und angewandte Mathematik, Bd. 145.
Druck und Verlag von Georg Reimer, Berlin.

MEINEN LIEBEN ELTERN

ZUR SILBERNEN HOCHZEIT

Digitized by the Internet Archive
in 2026

https://archive.org/details/IA41554030_0059

Einleitung.

Seit langem sind in die Arithmetik neben den sogenannten Körpern, in denen alle gewöhnlichen Rechengesetze wie für die rationalen Zahlen gelten, auch verschiedene Bereiche von Elementen eingeführt worden, die so umfassend und so in sich abgeschlossen sind, daß zwar Addition, Subtraktion und Multiplikation in ihnen unbeschränkt und eindeutig und auch in Übereinstimmung mit allen oder doch den wichtigsten formalen Gesetzen der Arithmetik ausgeführt werden können, aber die Division überhaupt nicht allgemein oder nicht immer eindeutig möglich ist. Das trivialste Beispiel eines solchen, mit Herrn *Hilbert* als *Ring**) zu bezeichnenden Bereiches stellt jedes Kongruenzklassensystem für eine beliebige zusammengesetzte natürliche Zahl als Modul dar; als einige weitere Beispiele derartiger Ringe seien verschiedene Arten von Systemen höherer komplexer Zahlen**) genannt, ferner Ringe von Matrizen oder von Modulsystemen

---

*) Eine nähere Präzisierung dessen, was — etwas abweichend von Herrn *Hilbert* — im nachfolgenden Aufsatz unter einem Ring verstanden wird, ist in § 1 gegeben.

**) Man vergleiche besonders eine Abhandlung von *Weierstraß* (mit zusätzlichen Bemerkungen von Herrn *H. A. Schwarz*; Nachr. v. d. K. Ges. d. Wiss. zu Göttingen, a. d. Jahre 1884, S. 395—419 [= *Weierstraß*' Mathem. Werke, II, S. 311—337]) sowie die sich daran anschließenden Aufsätze der Herren *H. A. Schwarz* (ebenda, S. 516—519 bzw. S. 337—339 [= *Schwarz*' Ges. math. Abh., II, S. 346—349]), *Dedekind* (ebenda, a. d. J. 1885, S. 141—159; vgl. auch ebenda, a. d. J. 1887, S. 1—7), *Hölder* (ebenda, a. d. J. 1886, S. 241—244), *J. Petersen* (ebenda, a. d. J. 1887, S. 489—502), *Hilbert* (ebenda, math.-phys. Kl., a. d. J. 1896, S. 179—183) sowie besonders des Herrn *Study* (ebenda, math.-phys. Kl., a. d. J. 1898, S. 1—8), in denen eine spezielle Klasse von Systemen höherer komplexer Zahlen betrachtet wird, die in augenfälliger Weise in den Rahmen des nachfolgenden Aufsatzes fällt; man vgl. hierfür das „Schlußergebnis" auf S. 41. Zum Vergleich

und schließlich die Bereiche der g-adischen Zahlen*). Es ist übrigens wesentlich zu unterscheiden, ob die Ringeigenschaft nur künstlich oder aber natürlich ist, nämlich ob man durch „Quotientenbildung“ (d. h. Adjunktion von Elemente*paaren* wie bei der Einführung der rationalen Zahlen) die Division unbeschränkt ausführbar und den Ring, der alsdann nur ein Integritätsbereich war, zum Körper machen kann — oder nicht; nur die Bereiche der letzteren Art fallen unter die folgenden Betrachtungen, in denen zu der rein arithmetischen Unterscheidung zwischen ganzen und gebrochenen Elementen keine Veranlassung vorliegt; sie sind vor den Körpern dadurch „ausgezeichnet“, daß in ihnen ein Produkt sehr wohl Null sein kann, ohne daß einer der Faktoren verschwindet, daß die Null hier also eigentliche Teiler besitzt.

Da nun die Ringe nicht allein in der Zahlentheorie, sondern auch in anderen weiten Gebieten der Arithmetik eine wichtige Rolle spielen, so dürfte es als ein Problem von Bedeutung erscheinen, die Ringe im allgemeinen, unter möglichstem Verzicht auf die Benutzung spezieller Eigenschaften, in bezug auf ihre möglichen Typen und die in ihnen herrschenden allgemeinen algebraischen Gesetze zu untersuchen, ähnlich wie dies vor kurzem Herr *Steinitz* für die Körper unternommen und vollständig durchgeführt hat**). Hier zeigt sich aber sogleich bei den ersten Schritten eine wesentliche Schwierigkeit darin, daß wegen der nur beschränkten und im allgemeinen nicht eindeutigen Ausführbarkeit der Division und wegen der Existenz echter Teiler der Null die grundlegendsten

---

sei noch besonders auf den außerordentlich viel weiteren Umfang des Gebiets der hier behandelten Systeme „höherer komplexer Zahlen“ hingewiesen: als Koeffizienten der Haupteinheiten höherer komplexer Zahlen werden gewöhnlich (auch in den oben zitierten Aufsätzen) nur reelle oder gemeine komplexe Zahlen zugelassen, neuerdings besonders in amerikanischen Arbeiten auch Elemente eines beliebigen Körpers; im vorliegenden Aufsatz dagegen (vgl. das erwähnte Schlußergebnis) gehören die Koeffizienten jeder einzelnen Haupteinheit e_i je einem besonderen Bereich $\mathfrak{R}_i$ an und zwar nicht notwendig einem Körper, sondern allgemeiner einem einfachsten Ring $\mathfrak{R}_i$ von der Art, daß jeder Nullteiler von $\mathfrak{R}_i$ im wesentlichen eine Potenz eines bestimmten, ein für allemal fest gewählten Nullteilers von $\mathfrak{R}_i$ ist.

*) Die g-adischen Zahlen hat Herr *Hensel* in die Arithmetik eingeführt in seiner jüngst erschienenen „Zahlentheorie“ (Berlin u. Leipzig [Göschen] 1913).

**) *E. Steinitz*: Algebraische Theorie der Körper, dieses Journal, Bd. 137 (1910), S. 167—309.

algebraischen Sätze und Methoden auf Ringe nicht ausgedehnt werden können; z. B. kann offenbar eine algebraische Gleichung mit Koeffizienten aus einem Ring in diesem sehr wohl mehr Wurzeln haben, als ihr Grad angibt, auch sogar unendlich viele Wurzeln.

Für die speziellen Ringe der g-adischen Zahlen hat nun Herr *Hensel* im fünften Kapitel seines erwähnten Buches diese Schwierigkeiten vollkommen beseitigt, indem er diese Ringe auf Grund ihrer besonderen Eigenschaften, namentlich auf Grund der Eigentümlichkeiten gewisser, explizit zu berechnender g-adischer Zahlen, auf jeweils endlichviele Körper zurückzuführen lehrte. Durch diese interessanten Ergebnisse angeregt, versuchte ich, ob nicht auch für die allgemeinen Ringe eine ähnliche Reduktion und damit ein Eingangsweg für weitere Untersuchungen ermöglicht werden könne. In der Tat zeigte sich, daß für eine sehr weite, durch abstrakte Bedingungen festgelegte Klasse von Ringen mittels allgemeiner Methoden eine Zurückführung geleistet werden kann zwar im allgemeinen nicht auf Körper, aber auf spezielle, durch einfache Struktur ausgezeichnete Ringe, in denen sich insbesondere alle Fragen der Division ohne weiteres entscheiden lassen (vgl. die Sätze 7 ff. des § 4 auf S. 38 ff.).

Der Durchführung dieser Untersuchung ist der folgende Aufsatz gewidmet, dem zur leichteren Übersicht über die sich in größerer Anzahl als notwendig erweisenden neuen Begriffsbildungen ein *Verzeichnis der Termini* angefügt ist. Zur Erläuterung der zuweilen der Natur der Sache nach etwas abstrakten Gedankengänge und der manchmal paradox erscheinenden Verhältnisse in Ringen sind häufig kurze Beispiele eingefügt; dagegen wurde von eigentlichen Anwendungen auf spezielle Ringe Abstand genommen, weil dies meist längere Hilfsbetrachtungen erfordern würde und daher besser einer anderen Gelegenheit vorbehalten bleibt. Mittels der Ergebnisse dieser Arbeit hoffe ich die nähere Untersuchung der Ringe in dem früher angegebenen Sinn bei nächster Gelegenheit weiter fortsetzen zu können.

§ 1. Die Ringe im allgemeinen.

Den Gegenstand aller nachfolgenden Betrachtungen bildet ein System $\mathfrak{R}$ von Elementen, in dem entweder irgend je zwei Elemente als untereinander ungleich gelten oder aber eine reflexive, symmetrische und tran-

sitive Relation = (Gleichheit) zwischen gewissen Elementen definiert ist, so daß also für jedes Element a aus $\mathfrak{R}$ stets $a = a$ gilt und, falls b und c ebenfalls Elemente aus $\mathfrak{R}$ sind, aus $a = b$ stets $b = a$, aus $a = b$, $b = c$ stets $a = c$ folgt. Im ersten Fall stellt die Identität eine solche Relation dar. Sind zwischen den Elementen des Systems auch noch Operationen, etwa eine Addition oder eine Multiplikation, definiert, so ist die Gleichheit als derart erklärt vorauszusetzen, daß bei diesen Operationen irgendwelche als gleich definierte Elemente einander vertreten können.

Ist im System $\mathfrak{R}$ eine beliebige Verknüpfungsoperation $\times$ zwischen je zwei Elementen definiert, so besage, wie üblich, die Ausdrucksweise „die Elemente von $\mathfrak{R}$ bilden in bezug auf die Operation $\times$ eine Gruppe“, daß die folgenden 4 Bedingungen*) erfüllt sind:

1. Aus irgend zwei in bestimmter Reihenfolge gegebenen Elementen a und b aus $\mathfrak{R}$ kann vermittels der Operation $\times$ eindeutig ein Element c gewonnen werden, das ebenfalls dem System $\mathfrak{R}$ angehört; es soll auch durch $c = a \times b$ bezeichnet werden.

2. Sind a, b, c irgend drei Elemente aus $\mathfrak{R}$, so ist stets $a \times (b \times c) = (a \times b) \times c$.

3. $\mathfrak{R}$ enthält mindestens ein Element n von der Art, daß für jedes Element a aus $\mathfrak{R}$ stets $a \times n = a$ ist.

4. Enthält $\mathfrak{R}$ Elemente von der in 3. geforderten Art, so gibt es unter ihnen ein besonderes $\bar{n}$ derart, daß $\mathfrak{R}$ zu jedem Element a mindestens ein Element a' enthält, für das $a \times a' = \bar{n}$ ist.

Diese Bedingungen sind unabhängig, gleichviel ob $\mathfrak{R}$ endlich oder unendlich viele Elemente enthält, und aus ihnen können alle Eigenschaften einer Gruppe gefolgert werden. Insbesondere sind die in 3. und 4. erklärten Elemente n und a' jeweils — abgesehen von zu ihnen gleichen Elementen — eindeutig bestimmt und sollen als neutrales Element

---

*) Diese Definition der Gruppe sowie ein Teil der zur Definition des Ringes verwendeten Bedingungen schließen sich an die Herren *Moore* und *Dickson* an (*Dickson* in den Transact. of the Amer. Math. Soc., Vol. 6 [1905], p. 198—204; vgl. auch die Darstellung in *Pascals* Repertor. der höh. Math., 2. Aufl., I. Bd., 1. Hälfte [Leipz. 1910], S. 172f., und in Herrn *Loewys* 1914 bei Veit & Comp. erscheinendem Lehrbuch: Algebra, I. Teil: Grundlagen d. Arithmetik, S. 24 ff. u. 33 ff., welch letzterem ich auch in der Darstellung der Gleichheit und öfters in diesem Paragraphen gefolgt bin).

der Gruppe bzw. als zu a inverses Gruppenelement gelegentlich bezeichnet werden.

Sind nur die ersten drei Bedingungen erfüllt, so werde $\mathfrak{R}$ als eine Paenegruppe*) bezeichnet.

Ein Ring heiße das System $\mathfrak{R}$, wenn die folgenden 10 Bedingungen $R_{1)}$ bis $R_{10)}$ erfüllt sind**):

$R_{1)}$ *Aus irgend zwei in bestimmter Reihenfolge gegebenen Elementen a und b aus $\mathfrak{R}$ kann vermittels einer Operation, die mit $+$ bezeichnet werde und Addition heiße, eindeutig ein Element c aus $\mathfrak{R}$ gewonnen werden, das auch als $c = a + b$ oder als Summe von a und b bezeichnet werden soll.*

$R_{2)}$ *Für irgend drei Elemente a, b, c aus $\mathfrak{R}$ ist stets $a + (b + c) = (a + b) + c$.*

$R_{3)}$ *$\mathfrak{R}$ enthält mindestens ein Element O von der Art, daß $a + O = a$ ist für jedes Element a aus $\mathfrak{R}$.*

$R_{4)}$ *Unter den Elementen O gibt es ein besonderes $\bar{O}$ von der Art, daß $\mathfrak{R}$ zu jedem Element a mindestens ein Element $(-a)$ enthält, für das $a + (-a) = \bar{O}$ ist.*

Diese vier ersten Bedingungen besagen, daß $\mathfrak{R}$ in bezug auf die Addition eine Gruppe bildet; das in bezug auf die Addition neutrale Element O***) werde als das Nullelement oder die Null des Systems $\mathfrak{R}$ bezeichnet.

---

*) Nicht zu verwechseln mit dem von Herrn *Dickson* (Transact. of the Amer. Math. Soc., vol. 6 [1905], p. 205) eingeführten Begriff der Halbgruppe (semi-group).

**) Die Bedingungen sind des leichteren Vergleichs wegen so formuliert, daß $R_{1)}$ bis $R_{7)}$ und $R_{10)}$ mit den entsprechenden Körperbedingungen bei *Dickson* und *Loewy* identisch, $R_{8)}$ und $R_{9)}$ den entsprechenden analog sind; $R_{1)}$ bis $R_{4)}$ besagen, daß die Elemente von $\mathfrak{R}$ in bezug auf die Addition eine Gruppe bilden, $R_{5)}$ bis $R_{8)}$, daß sie in bezug auf die Multiplikation *möglichst*, nämlich nach Ausschluß der Nullteiler, eine Gruppe bilden. *Einschränkender Natur* sind von den 10 Bedingungen nur $R_{7)}$, $R_{8)}$ und $R_{9)}$; $R_{8)}$ schließt bei kommutativer Multiplikation nur die in der Einleitung als „künstlich“ bezeichneten Ringe aus und ist dann durch Quotientenbildung zu befriedigen, während $R_{7)}$ und $R_{9)}$ wesentliche Anforderungen stellen, welche zum mindesten nicht gänzlich weggelassen werden können, will man nicht zu einer ganz anderen und viel weniger weitgehenden Theorie gelangen als der im folgenden entwickelten.

***) Bei Elementen, die, abgesehen von zu ihnen gleichen, eindeutig bestimmt sind, soll stets in dieser Weise der bestimmte Artikel gebraucht und von eindeutiger Bestimmtheit schlechthin gesprochen werden.

Nach den bekannten Eigenschaften einer Gruppe gilt:

Satz 1: *Für Elemente a, b eines Ringes $\mathfrak{R}$ ist stets:* $a + O = O + a = a$, $a + (-a) = (-a) + a = O$, $-(a + b) = (-b) + (-a)$; *ferner gilt das assoziative Gesetz für die Addition beliebig vieler Elemente aus $\mathfrak{R}$ und schließlich ist jede Lösung der Gleichung $a + x = b$ bzw. $y + a' = b'$ aus $\mathfrak{R}$ gleich dem Element $x = (-a) + b$ bzw. $y = b' + (-a')$, d. h. die Addition ist eindeutig umkehrbar.* Für $a + (-b)$ werde kürzer $a - b$ geschrieben.

Die weiteren Bedingungen für einen Ring sind:

R_5) *Aus irgend zwei in bestimmter Reihenfolge gegebenen Elementen a und b aus $\mathfrak{R}$ kann vermittels einer Operation, die mit $\cdot$ bezeichnet werde und Multiplikation heiße, eindeutig ein Element c aus $\mathfrak{R}$ gewonnen werden, das auch als $c = a \cdot b$ oder als Produkt von a und b bezeichnet werden soll.*

R_6) *Für irgend drei Elemente a, b, c aus $\mathfrak{R}$ ist stets $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.*

R_7) *$\mathfrak{R}$ enthält mindestens ein Element ε von der Art, daß für jedes Element a aus $\mathfrak{R}$ $a \cdot \varepsilon = a$ ist;* ein solches Element ε heiße ein Einheitselement von $\mathfrak{R}$.

Definition 1: Gibt es zu einem Element b aus $\mathfrak{R}$ ein zweites $a \neq O$ in $\mathfrak{R}$, so daß $a \cdot b = O$ ist, so heiße mit *Weierstraß* b ein Teiler der Null oder ein Nullteiler. Ein Element aus $\mathfrak{R}$, das kein Nullteiler ist, werde als regulär bezeichnet.

Beliebige Elemente aus $\mathfrak{R}$ sollen im folgenden mit lateinischen, reguläre mit kleinen griechischen Buchstaben bezeichnet werden.

R_8) *Unter den Einheitselementen ε von $\mathfrak{R}$ gibt es ein besonderes $\bar{\varepsilon}$ von der Art, daß $\mathfrak{R}$ zu jedem regulären Element α mindestens ein Element α^{-1} enthält, für das $\alpha \cdot \alpha^{-1} = \bar{\varepsilon}$ ist. α^{-1} heiße ein zu α reziprokes Element.*

R_9) *Sind a und b irgend zwei Elemente aus $\mathfrak{R}$, so gibt es zu ihnen ein reguläres Element $\alpha_{a,b}$ in $\mathfrak{R}$, so daß $a \cdot b = \alpha_{a,b} \cdot b \cdot a$ ist, und ein reguläres Element $\beta_{a,b}$, so daß $a \cdot b = b \cdot a \cdot \beta_{a,b}$ ist. Die Multiplikation im Ring braucht also nicht kommutativ zu sein, aber $a \cdot b$ und $b \cdot a$ unterscheiden sich voneinander höchstens um einen vorne oder hinten hinzuzufügenden regulären Faktor.*

R_{10}) *Sind a, b, c irgend drei Elemente aus $\mathfrak{R}$, so gelten die distributiven Gesetze:*

$$a \cdot (b + c) = a \cdot b + a \cdot c, \quad (b + c) \cdot a = b \cdot a + c \cdot a.$$

Ist insbesondere in $\mathfrak{R}$ die Multiplikation kommutativ, so genügt es, *eines* der distributiven Gesetze zu fordern. $\mathfrak{R}$ heiße in diesem Fall ein kommutativer Ring.

Fügt man noch die Bedingung hinzu, daß ein Produkt nur dann verschwinde, wenn dies von einem der Faktoren gilt, oder, was dasselbe ist, daß zu *jedem* zu Null ungleichen Element ein reziprokes in $\mathfrak{R}$ existieren solle, so geht bekanntlich ein kommutativer Ring $\mathfrak{R}$ in einen Körper über; ist die Multiplikation in einem derartigen Ring nicht kommutativ — in diesem Fall wird übrigens die Bedingung $R_{9)}$ überflüssig —, so will ich mit den Herren *Zermelo* und *Blumberg**) von einem nichtkommutativen Körper sprechen.

In einem Ring bilden die Elemente auch bei Ausschluß der Null keine Gruppe in bezug auf die Multiplikation, sondern nur eine Paenegruppe, und es gelten in der Tat die dem Satze 1 analogen Behauptungen nicht sämtlich für die Multiplikation in Ringen. Doch folgt noch auf gleiche Weise wie für Körper:

Satz 2: *Für jedes Element a eines Ringes $\mathfrak{R}$ ist $a \cdot O = O \cdot a = O$; für irgend zwei Elemente a und b aus $\mathfrak{R}$ ist:*

$$a \cdot (-b) = (-a) \cdot b = -(a \cdot b), \quad (-a) \cdot (-b) = a \cdot b.$$

Enthält $\mathfrak{R}$, wie zur Vermeidung von Trivialitäten stets angenommen werden soll, wenigstens ein zu O ungleiches Element, so sind Addition und Multiplikation verschiedene Operationen, und jedes Einheitselement ist ungleich Null. Das assoziative Gesetz gilt für die Multiplikation beliebig vieler Elemente aus $\mathfrak{R}$.

Aus $R_{9)}$ und der ersten Behauptung von Satz 2 folgt noch, daß auch *a ein Nullteiler ist, wenn $a \cdot b = O$ und $b \neq O$ ist;* eine Unterscheidung zwischen Nullteilern der ersten und der zweiten Art braucht hier also nicht gemacht zu werden.

Satz 3: *Die Addition ist in jedem Ring kommutativ. Auch bei der Multiplikation endlichvieler Faktoren aus einem Ring darf die Reihenfolge beliebig geändert werden, wenn nur vorn oder hinten ein geeignet gewählter regulärer Faktor hinzugefügt wird. Die vordere multiplikative Hinzu-*

*) Vgl. Bull. of the Amer. Mathem. Soc., vol. 19 (1913), p. 58f..

fügung eines Einheitselements läßt ebenso wie die hintere jedes Ringelement ungeändert; das Einheitselement eines Ringes ist daher eindeutig bestimmt. Ein Ring enthält zu keinem Nullteiler ein reziprokes Element, und die Gesamtheit aller regulären Elemente eines Ringes bildet in bezug auf die Multiplikation eine Gruppe.

Beweis: Sind a und b zwei beliebige Elemente eines Ringes $\mathfrak{R}$, ε ein Einheitselement von $\mathfrak{R}$, so ist nach dem ersten distributiven Gesetz

$$(a+b)\cdot(\varepsilon+\varepsilon)=a+b+a+b,$$

nach dem zweiten

$$(a+b)\cdot(\varepsilon+\varepsilon)=a\cdot(\varepsilon+\varepsilon)+b\cdot(\varepsilon+\varepsilon)=a+a+b+b,$$

so daß nach Satz 1 in der Tat folgt: $a+b=b+a$, was sich in bekannter Weise auf mehr als zwei Summanden überträgt. Weiter ist nach $R_{7)}$ und $R_{9)}$: $a=a\cdot\varepsilon=\varepsilon\cdot a\cdot\beta_{a,\varepsilon}$, woraus durch vordere Multiplikation mit ε die zu beweisende Relation $\varepsilon\cdot a=a$ folgt. Ferner sei $a\cdot b=O=b\cdot a$, aber $b\neq O$; existierte dann a^{-1} so, daß $a\cdot a^{-1}=\varepsilon$ wäre, so folgte $O=b\cdot a\cdot a^{-1}=b\cdot\varepsilon=b$ gegen die gemachte Voraussetzung, d. h. Nullteiler besitzen wirklich keine Reziproken. Das Produkt zweier regulärer Elemente $\alpha\cdot\beta$, zu dem ja $\beta^{-1}\cdot\alpha^{-1}$ reziprok ist, ist daher wieder regulär, woraus mit Rücksicht auf $R_{6)}$, $R_{7)}$ und $R_{8)}$ die letzte Behauptung von Satz 3 folgt. Aus dieser schließlich ergibt sich bei wiederholter Anwendung von $R_{9)}$ die Richtigkeit der Aussage über die Veränderung der Reihenfolge der Faktoren bei der Multiplikation.

Die natürlichen *Potenzen* eines Ringelements, die mehrfach vorkommen werden, seien gleich hier in bekannter Weise eingeführt durch die Definitionen

$$a=a^1,\quad a^m\cdot a=a^{m+1},$$

wo a ein beliebiges Element aus $\mathfrak{R}$, dagegen $1, 2, \ldots m, \ldots$ nur abkürzende Symbole und nicht etwa Ringelemente sind*); die gewöhnlichen Rechenregeln wie $a^m\cdot a^n=a^{m+n}$ usw. sind leicht herzuleiten. Gelegentlich wird auch die Schreibweise $a^0=\varepsilon$ benutzt werden.

*) Auch die Addition dieser Symbole hat natürlich mit der im Ring definierten Addition nichts zu tun; die Benutzung der gewöhnlichen Operationszeichen für die Addition, Subtraktion und Multiplikation ganzer Zahlen wird an den wenigen Stellen, wo sie auftreten, zu Mißverständnissen wohl nicht führen.

Es sei auch hier schon als Beispiel eine höchst einfache Klasse von Ringen angeführt, von der später zur Illustration der einzelnen Sätze und Gedankengänge ausgiebiger Gebrauch gemacht werden soll. m sei eine beliebige natürliche Zahl >1; dann betrachte ich die Klassen derjenigen ganzen Zahlen (oder allgemeiner rationalen Zahlen mit zu m teilerfremden Nennern in der reduzierten Form), die der Reihe nach den Zahlen $0, 1, 2, \ldots m-1$ modulo m kongruent sind, und bezeichne auch diese Klassen selbst gleich mit $0, 1, \ldots m-1$. Wird die Addition, Subtraktion, Multiplikation und, soweit möglich, auch die Division dieser Klassen in der gewöhnlichen Weise, nur stets modulo m, ausgeführt, so hat man in dem System dieser Klassen einen Ring, der allen Bedingungen $R_{1)}$ bis $R_{10)}$ genügt, den Ring R_m der Kongruenzklassen modulo m. Er ist dann und nur dann ein Körper, wenn m eine Primzahl ist, in jedem andern Fall aber ein kommutativer Ring, der außer der Null noch weitere Nullteiler enthält. Z. B. sind in R_{360} alle und nur die Klassen Nullteiler, die durch mindestens einen der Primfaktoren 2, 3, 5 von 360 teilbar sind; so sind etwa 5 und 72 Nullteiler, weil $5 \cdot 72 = 0$ und $72 \neq 0$, $5 \neq 0$ ist.

Definition 2: Ist $a = b \cdot c$, wo a, b, c Elemente eines Ringes $\mathfrak{R}$ bedeuten, so heißt a durch c teilbar, c ein Teiler von a oder in a enthalten usw.. — Ist allgemeiner $a = b \cdot c \cdot d$, so ist ebenfalls a durch c teilbar; denn nach $R_{9)}$ ist: $a = b \cdot c \cdot d = b \cdot \alpha_{c,d} \cdot d \cdot c$.

Definition 3: Ist sowohl a durch b wie auch b durch a teilbar, so heißen a und b unwesentlich verschieden oder äquivalent ($a \backsim b$); in jedem andern Fall heißen a und b wesentlich verschieden. Ist insbesondere a durch b, aber b nicht durch a teilbar, so heißt b ein echter Teiler von a.

Die so definierte Äquivalenz ist offenbar reflexiv, symmetrisch und transitiv. Alle regulären Elemente sind untereinander, also speziell auch mit dem Einheitselement äquivalent.

Z. B. ist in R_{360} $25 \backsim 5$ und $7 \backsim 1$, weil $25 = 5 \cdot 5$, $5 = 29 \cdot 25$ und $7 = 7 \cdot 1$, $1 = 103 \cdot 7$ ist. Dagegen sind 2 und 4 wesentlich verschieden, weil 2 durch 4 nicht teilbar ist; da andererseits $4 = 2 \cdot 2$ ist, so ist 2 ein echter Teiler von 4.

Satz 4: *Unterscheiden sich a und b nur um reguläre Faktoren, so ist $a \backsim b$.*

Denn aus $\alpha_1 \cdot a \cdot \alpha_2 = \beta_1 \cdot b \cdot \beta_2$ folgt:

$$a = \alpha_1^{-1} \cdot \beta_1 \cdot b \cdot \beta_2 \cdot \alpha_2{}^1, \quad b = \beta_1^{-1} \cdot \alpha_1 \cdot a \cdot \alpha_2 \cdot \beta_2{}^1.$$

Die außerordentlich viel tiefer liegende Umkehrung dieses Satzes wird erst viel später und nur für eine besondere Klasse von Ringen bewiesen werden (Satz 6 des § 3 auf S. 33).

Definition 4: Ein Ring heiße endlich oder von der endlichen Ordnung m*), wenn die Zahl seiner ungleichen Elemente endlich und zwar gleich m ist; enthält er unendlich viele ungleiche Elemente, so heiße er unendlich oder von unendlich hoher Ordnung.

Definition 5: Ein Ring heiße von endlichem Grade n, wenn die Zahl seiner *wesentlich verschiedenen* Elemente endlich und zwar gleich n ist; enthält er unendlich viele wesentlich verschiedene Elemente, so heiße er von unendlich hohem Grad.

Während jeder endliche Ring endlichen Grad besitzt, kann natürlich ein Ring von endlichem Grad sehr wohl eine abzählbar unendliche oder größere Mächtigkeit von Elementen besitzen. Z. B. ist nicht nur jeder Ring von Kongruenzklassen für irgendeinen Modul, sondern auch der Ring der rationalen g-adischen Zahlen für irgendeine natürliche Zahl g**) von endlichem Grad, nämlich vom Grad 2^n, wenn n die Anzahl der verschiedenen Primfaktoren von g bezeichnet, ebenso jeder Ring algebraischer g-adischer Zahlen; dagegen besitzt die Menge aller *ungleichen* Elemente dieser Ringe die Mächtigkeit des Kontinuums. Jeder Ring unendlich hohen Grades enthält (sogar unendlich viele wesentlich verschiedene) Elemente (z. B. die Null), welche durch unendlich viele wesentlich verschiedene Nullteiler teilbar sind.

Zum Schluß dieses Paragraphen soll noch gezeigt werden, daß die Bedingungen $R_{1)}$ bis $R_{10)}$, durch die ein Ring definiert wurde, untereinander unabhängig sind. Da alle 10 Bedingungen stets erfüllt sind für Körper, in denen ja die Multiplikation kommutativ ist und durch jedes von Null verschiedene Element dividiert werden kann, so wird die Unabhängigkeit jeder der Bedingungen $R_{1)}$ bis $R_{8)}$ sowie $R_{10)}$ von den neun übrigen gewährleistet durch die Pseudokörper, welche man zum Nachweis der Unabhängigkeit der entsprechenden Körperbedingungen konstruiert hat***). Es ist daher nur mehr die Unabhängigkeit der Bedingung $R_{9)}$ von den übrigen zu zeigen.

Zu diesem Zweck betrachte ich das System aller „Quaternionen“

*) Etwas speziellere Ringe endlicher Ordnung sind jüngst von Herrn *H. S. Vandiver* auf einige Eigenschaften hin untersucht worden: Transact. of the Amer. Math. Soc., vol. 13 (1912), p. 293—304.

**) Über die g-adischen Zahlen vgl. *K. Hensel*: Zahlentheorie (Berl. u. Leipz. 1913).

***) Vgl. *Dickson*, a. a. O., p. 202—204, oder *Loewys* zitiertes Lehrbuch, S. 52—54.

der Form $a_0 + 2a_1 i_1 + 2a_2 i_2 + 2a_3 i_3$, wobei die a_i beliebige Werte eines vollständigen Restsystems modulo 8, z. B. der Reihe 0, 1, ... 7, unabhängig voneinander annehmen können. Addition und Multiplikation sind stets modulo 8 auszuführen, sonst aber in der gewöhnlichen Weise, wonach im besonderen auch jedes Quaternion mit jeder Zahl multiplikativ vertauschbar ist; für die Produkte der Haupteinheiten i_1, i_2, i_3 sind die aus nebenstehender Tabelle hervorgehenden Werte einzusetzen, wobei aber zu beachten ist, daß i_1, i_2, i_3 selbst gar nicht Elemente des Systems sind (für sie würde das assoziative Gesetz der Multiplikation nicht allgemein gelten).

Werte von $u \cdot v$

u \ v	i_1	i_2	i_3
i_1	2	i_3	$2i_2$
i_2	$2i_3$	2	i_1
i_3	i_2	$2i_1$	2

Dagegen sei $8i_1 = 8i_2 = 8i_3 = 0$. Für dieses System sind alle Bedingungen außer $R_{9)}$ erfüllt; Nullteiler sind alle und nur die Elemente $a_0 + 2a_1 i_1 + 2a_2 i_2 + 2a_3 i_3$, für die a_0 durch 2 teilbar ist, und zu jedem anderen existiert das eindeutig bestimmte reziproke Element

$$a_0' + 2a_0'^3(2a_2a_3 - a_0a_1)i_1 + 2a_0'^3(2a_3a_1 - a_0a_2)i_2 + 2a_0'^3(2a_1a_2 - a_0a_3)i_3,$$

wo $a_0 a_0' \equiv 1 \pmod 8$. Dagegen ist $R_{9)}$ nicht erfüllt; denn es ist z. B. $2i_1 \cdot 2i_2 = 4i_3$, dagegen $2i_2 \cdot 2i_1 = 0$.

§ 2. Die zerlegbaren Ringe, ihre Primteiler und Primärteiler der Null und die multiplikative Zerlegung ihrer Elemente.

Definition 1: Gegeben sei ein beliebiger Ring $\mathfrak{R}$; ein Nullteiler aus $\mathfrak{R}$, der außer regulären Elementen keinen echten Teiler besitzt, in dem also nur ihm äquivalente und reguläre Elemente enthalten sind, heiße ein Primteiler der Null oder auch kurz ein Primteiler.

Beispiel für R_{360}: Primteiler von R_{360} sind alle Klassen, die entweder durch 2, aber durch keine höhere Potenz von 2 und weder durch 3 noch durch 5 — oder durch 3, aber durch keine höhere Potenz von 3 und weder durch 2 noch durch 5 — oder durch eine beliebige Potenz von 5, aber weder durch 2 noch durch 3 teilbar sind, also die Klassen

2, 14, 22, 26, 34, ...; 3, 21, 33, 39, 51, ...;
5, 25, 35, 55, 65, ...

Z. B. ist 25 ein *Primteiler* der Null; denn es ist zwar $25 = 5 \cdot 5$, aber 5 ist kein *echter* Teiler von 25, weil auch $5 = 25 \cdot 29$. Die Primteiler jeder der drei Kategorien sind jeweils untereinander äquivalent.

Satz 1: *Ist $\mathfrak{R}$ ein Ring von endlichem Grad, so enthält jeder Nullteiler a aus $\mathfrak{R}$ mindestens einen Primteiler.*

Denn ist a nicht selbst Primteiler, so enthält a wegen der Definition der Primteiler einen echten Teiler a_1, der nicht regulär ist. Ist a_1 Primteiler, so ist der Satz für a zutreffend; im anderen Fall muß ebenso a_1 einen echten, nicht regulären Teiler a_2 enthalten, der nicht nur von a_1, sondern auch von a wesentlich verschieden ist. Setzt man das Verfahren fort, so muß man schließlich, da $\mathfrak{R}$ nach Voraussetzung nur endlich viele wesentlich verschiedene Nullteiler enthält, zu einem in a enthaltenen Primteiler gelangen, w. z. b. w.*).

Satz 2: *Jeder einem Ringe $\mathfrak{R}$ angehörige Nullteiler a, der kein Primteiler ist, aber einen solchen enthält — wie letzteres in Ringen endlichen Grades für alle Nullteiler zutrifft —, läßt sich in ein Produkt $a = a_1 \cdot a_2$ in $\mathfrak{R}$ zerlegen, in dem beide Faktoren a_1 und a_2 von a wesentlich verschieden sind.*

Beweis: p sei ein in a enthaltener Primteiler, so daß etwa $a = a_1 \cdot p$ ist. Ist a_1 nicht durch a teilbar, so ist der Satz bewiesen. Es sei daher $a_1 = a_2 \cdot a$; ferner sei $P \cdot p = O$, wo $P \neq O$ (ein solches Element P muß in $\mathfrak{R}$ existieren, weil p ein Nullteiler von $\mathfrak{R}$ ist). Dann ist sicher P nicht teilbar durch a, weil aus $P = b \cdot a$ folgen würde:

$$P = b \cdot a = b \cdot a_2 \cdot a \cdot p = b \cdot a \cdot p \cdot a_2 \cdot \beta_{a_2, a \cdot p} \text{ (vgl. } R_{9)} \text{ a. S. 10)}$$
$$= P \cdot p \cdot a_2 \cdot \beta_{a_2, a \cdot p} = O \text{ gegen die Voraussetzung.}$$

Nun ist:

$$a = a + P \cdot p = (a_1 + P) \cdot p;$$

hier aber ist sicher $a_1 + P$ von a wesentlich verschieden, weil mit $a_1 + P$ zugleich auch $P = a_1 + P - a_2 \cdot a$ durch a teilbar wäre; der Satz ist also bewiesen.

Beispiel für R_{360}: $a = 40$, $a_1 = 80$, $p = 5$, $a_2 = 2$, $P = 72$. Es ist $40 = 80 \cdot 5$, $80 = 2 \cdot 40$; aus $72 \cdot 5 = 0$ folgt daher: $40 = (80 + 72) \cdot 5 = 152 \cdot 5$, wo 152 ein echter Teiler von 40 ist.

Es sei nun $\mathfrak{R}$ von endlichem Grade, a ein Nullteiler aus $\mathfrak{R}$, der nicht schon selbst ein Primteiler ist, und es sei nach Satz 2 $a = a_1 \cdot a_2$, wo weder a_1 noch a_2 äquivalent a ist. Ebenso lassen sich dann a_1 und a_2 als Produkte eigentlicher Teiler ($a_1 = a_{11} \cdot a_{12}$, $a_2 = a_{21} \cdot a_{22}$) darstellen, falls weder a_1 noch a_2 ein Primteiler ist. Bei jedem folgenden Schritt des in dieser Weise weiter fortsetzbaren Verfahrens gelangt man so zu einer Reihe von

*) Diese Methode reicht zwar zum Beweis von Satz 1 hin, nicht aber wie bei der Zerlegung der natürlichen Zahlen in Primfaktoren zum Beweis der Sätze 2 und 3.

(nicht notwendig verschiedenen) Nullteilern, deren jeder ein echter Teiler eines gewissen Elements der vorhergehenden Reihe ist, falls dieses nicht schon ein Primteiler war. Da $\mathfrak{R}$ nur endlichviele wesentlich verschiedene Nullteiler enthält, so muß das Verfahren schließlich zu lauter Primteilern führen. Bedenkt man noch, daß vermöge $\varepsilon \cdot O = O$, $\varepsilon \neq O$ die Null eines jeden Ringes ein Nullteiler ist, in einem (auch nichtkommutativen) Körper aber ein Produkt nur zugleich mit einem seiner Faktoren verschwindet, so hat man:

Satz 3: *Jeder endliche oder unendliche Ring endlichen Grades enthält eine positive endliche Anzahl wesentlich verschiedener Primteiler der Null; dann und nur dann ist die Null selbst ein Primteiler — und zwar dann der einzige —, wenn der Ring ein (eventuell nichtkommutativer) Körper ist. Jeder Nullteiler eines Ringes von endlichem Grade läßt sich auf mindestens eine Weise als Produkt endlich vieler Primteiler der Null darstellen.*

Beispiel für R_{360}: Eine Zerlegung von 60 in Primteiler der Null ist: $60 = 2 \cdot 30 = 2 \cdot 25 \cdot 174 = 2 \cdot 25 \cdot 58 \cdot 3$.

Offenbar ist in Ringen von Kongruenzklassen diese Zerlegung in Primteiler der Null sogar bis auf die Reihenfolge *eindeutig*, wenn man äquivalente Primteiler nicht als verschieden ansieht (dabei ist allerdings noch vorauszusetzen, daß überflüssige Faktoren beseitigt sind). In dem geführten Beweis ist jedoch nichts hierüber enthalten und eine solche wichtige Eigenschaft wird denn auch bei den allgemeinsten Ringen gar nicht zu erwarten sein. Daß man in der Tat noch eine besondere Forderung zu stellen hat, will man sich auf Ringe beschränken, bei denen die Zerlegung einer derartigen Eindeutigkeitsbedingung genügt, das läßt sich z. B. mittels des auf S. 14f. (zum Nachweis der Unabhängigkeit der Ringbedingung R_9)) benutzten Systems von „Quaternionen“ erkennen, wenn man es nur dahin abändert, daß die Multiplikation kommutativ bleibt.

Man betrachte also wieder einen Ring von Elementen der Form $a_0 + 2a_1 i_1 + 2a_2 i_2 + 2a_3 i_3$, wo $a_i = 0, 1, \ldots 7$ und sowohl die Addition wie die Multiplikation modulo 8 auszuführen ist und kommutativ sein soll. Die Produkte der — wieder im Ring selbst nicht vorkommenden — Haupteinheiten i_1, i_2, i_3 sind nach der vorstehenden Tabelle zu bilden;

Werte von $u \cdot v$:

$u = \downarrow$ / $v = \rightarrow$	i_1	i_2	i_3
i_1	2	i_3	i_2
i_2	i_3	2	i_1
i_3	i_2	i_1	2

es sei wieder $8i_1 = 8i_2 = 8i_3 = 0$. Dann sind $2, 2i_1, 2i_2, 2i_3$ wesentlich verschiedene Primteiler des Ringes; trotzdem ist z. B. $4i_1 = 2 \cdot 2i_1 = 2i_2 \cdot 2i_3$, d. h. man hat zwei wesentlich verschiedene Zerlegungen von $4i_1$ in Primteiler.

Um daher diejenigen Ringe, für deren Elemente eine gewisse, später näher zu präzisierende *Eindeutigkeit* der Zerlegung in Primteiler der Null besteht, unter den ganz allgemeinen Ringen hervorzuheben, dient die folgende

Definition 2: Ein Ring $\mathfrak{R}$ von endlichem oder unendlich hohem Grad heiße zerlegbar, wenn er außer den Bedingungen $R_{1)}$ bis $R_{10)}$ auch noch die folgende Z) erfüllt:

Z) *Sind a, b, c Elemente aus $\mathfrak{R}$ und ist $a \cdot b$ durch c teilbar, so läßt sich c auf mindestens eine Weise als Produkt $c = c_1 \cdot c_2$ derart darstellen, daß a durch c_1 und b durch c_2 teilbar ist.*

Die Bedingung ist in dieser Weise formuliert, um bei der Definition der zerlegbaren Ringe diejenige der Primteiler der Null nicht voraussetzen zu müssen. Das genaue Analogon der Bedingung Z) wird z. B. von den gewöhnlichen ganzen rationalen Zahlen erfüllt, nicht aber von den ganzen Zahlen jedes beliebigen algebraischen Zahlkörpers, in dem eben in der Tat die Zerlegung in Primfaktoren nicht notwendig eindeutig ist.

Über die Zerlegbarkeit der Ringe endlichen Grades, die in diesem Paragraphen bisher ausschließlich betrachtet wurden, gibt das folgende *hinreichende Kriterium* Aufschluß, das im allgemeinen sehr viel einfacher als die Bedingung Z) nachzuprüfen sein wird:

Satz 4: *Lassen sich in einem Ring $\mathfrak{R}$ von endlichem Grad zu jedem gegebenen Paar wesentlich verschiedener Primteiler der Null aus $\mathfrak{R}$, p_1 und p_2, zwei reguläre Elemente α_1 und α_2 finden, so daß $\alpha_1 \cdot p_1 + \alpha_2 \cdot p_2$ regulär wird, so ist $\mathfrak{R}$ ein zerlegbarer Ring.*

Da $(\alpha_1 \cdot p_1, \alpha_2 \cdot p_2)$ wieder ein Paar von Primteilern ist, demgegenüber (p_1, p_2) in keiner Weise ausgezeichnet ist, so kann man auch kurz sagen: Ein Ring endlichen Grades ist zerlegbar, wenn die Summe je zweier wesentlich verschiedener, passend gewählter Primteiler regulär ist.

Beispiel für den Ring R_{105} der Kongruenzklassen modulo 105: Es ist (3, 5, 7) ein vollständiges System wesentlich verschiedener Primteiler der Null aus R_{105}; da

z. B. $3+5=8$ (regulär), $100+7=2$ (regulär) und $9+49=58$ (regulär) ist, wobei die Äquivalenzen $9 \sim 3$, $100 \sim 5$, $49 \sim 7$ gelten, so ist R_{105} (wie jeder solche Ring von Kongruenzklassen) zerlegbar.

Zum Beweis des Satzes 4 dient wesentlich folgender

Hilfssatz: *Ist $\mathfrak{R}$ ein endlicher Ring, der die Voraussetzung des Satzes 4 erfüllt, so ist ein Produkt $a \cdot b$ aus $\mathfrak{R}$, dessen einer Faktor a genau durch die m-te ($m = 0, 1, 2, \ldots$), aber durch keine höhere Potenz eines bestimmten Primteilers p teilbar ist, während im andern Faktor b überhaupt p nicht enthalten ist, selbst nur durch p^m und keine höhere Potenz von p teilbar.*

Daß mit diesem Satz zugleich auch Satz 4 bewiesen sein wird, daß also die in dem Hilfssatz ausgesprochene Eigenschaft in endlichen Ringen die Zerlegbarkeit, aus der sie ja ohne weiteres folgt, auch umgekehrt nach sich zieht, leuchtet fast unmittelbar ein; der Gedankengang soll hier nur skizziert werden. Das in der Bedingung Z) (S. 18) auftretende Element c habe zunächst die Eigenschaft, nicht zwei wesentlich verschiedene Primteiler der Null zu enthalten; dann ist, wenn c im besonderen regulär ist, die Zerlegbarkeitsbedingung sicher erfüllt. Durch vollständige Induktion folgt, wenn man die Eigenschaft des Hilfssatzes als bewiesen betrachtet, das nämliche noch für den Fall, daß c sich als Produkt äquivalenter Primteiler darstellen läßt; man hat hierzu von den Fällen, wo eine der nach Satz 3 möglichen Zerlegungen von c genau $n-1$ ($n = 1, 2, \ldots$) äquivalente Primteiler, keine aber mehr enthält, aufzusteigen zu denjenigen Fällen, in denen mindestens *eine* solche Zerlegung genau n äquivalente Primteiler besitzt. Enthält schließlich c zwei oder mehr wesentlich verschiedene Primteiler, so benutze man wieder eine Zerlegung von c nach Satz 3; auf Grund der vorausgesetzten Eigenschaft des Hilfssatzes folgt dann unmittelbar aus dem Erfülltsein der Zerlegbarkeitsbedingung für jedes in c vorkommende Produkt äquivalenter Primteiler, daß auch c selbst jene Bedingung befriedigt.

Dem jetzt zu führenden Beweis des Hilfssatzes sei noch folgende Bemerkung vorangeschickt: Das in ihm vorkommende Element b kann ersichtlich als so gewählt vorausgesetzt werden, daß für keinen *echten* Teiler b_0 von b sich $a \cdot b_0$ von $a \cdot b$ nur unwesentlich unterscheidet (was bei Nullteilern sehr wohl möglich ist; z. B. für R_{105}: $a = 15$, $b = 35$, $b_0 = 7$); denn in diesem Fall genügt es, von vornherein $a \cdot b_0$ zu betrachten, da der zu beweisende Satz, wenn er für dieses Produkt zutrifft, für $a \cdot b$

a fortiori richtig ist. Ferner sei bemerkt, daß offenbar, falls α ein reguläres Element bedeutet, $\alpha \cdot b$ und $b \cdot \alpha$ nur durch die Teiler von b teilbar sind, weil ja von $\alpha^{-1} \cdot \alpha \cdot b$ bzw. $b \cdot \alpha \cdot \alpha^{-1}$ das nämliche gilt.

Der Beweis des Hilfssatzes selbst ist jetzt durch vollständige Induktion zu führen. Der Satz ist nämlich ersichtlich stets richtig für alle Produkte $a \cdot b$, die regulär sind, oder zwar *einen* Nullteiler, aber keinen von ihm wesentlich verschiedenen enthalten. Er sei bereits bewiesen für alle Produkte $a \cdot b$, die durch weniger als n wesentlich verschiedene Nullteiler teilbar sind. Dann ist zwar sehr wohl denkbar, daß überhaupt kein Produkt $a \cdot b$ aus $\mathfrak{R}$ genau n wesentlich verschiedene Nullteiler enthält; jedenfalls aber muß es — falls in dem Ring überhaupt n wesentlich verschiedene Nullteiler vorkommen — Produkte $a \cdot b$ mit n oder mehr wesentlich verschiedenen nicht regulären Teilern derart geben, daß jedes Element aus $\mathfrak{R}$, das weniger wesentlich verschiedene Teiler als $a \cdot b$ besitzt, höchstens $n - 1$ solche enthält. Angenommen nun, ein Produkt $a \cdot b$ von jener letztgenannten Art wäre durch p_1^{m+1} teilbar, während in a nur p_1^m, in b der Primteiler p_1 überhaupt nicht enthalten wäre; dann sei p_2 ein beliebiger in b enthaltener, also von p_1 wesentlich verschiedener Primteiler (für reguläres b wäre ja die Annahme ohne weiteres absurd), und es seien α_1 und α_2 gemäß der Voraussetzung des Satzes 4 solche reguläre Elemente aus $\mathfrak{R}$, daß $\alpha_1 \cdot p_1 + \alpha_2 \cdot p_2$ regulär ist. Ferner sei $b = b_0 \cdot p_2$, wo b nicht auch in b_0 enthalten sei; nach dem beim Beweis des Satzes 2 (S. 16) eingeschlagenen Verfahren läßt sich ein solches Element b_0 stets ermitteln. Dann ist

$$b + b_0 \cdot \alpha_2^{-1} \cdot \alpha_1 \cdot p_1 = c = b_0 \cdot \alpha_2^{-1} \cdot (\alpha_2 \cdot p_2 + \alpha_1 \cdot p_1) = b_0 \cdot \alpha_2^{-1} \cdot \eta ,$$

wo η ebenso wie α_2^{-1} nach Voraussetzung regulär, c also nicht durch p_1 teilbar ist. Es wäre aber

$$a \cdot c = a \cdot b + a \cdot b_0 \cdot \alpha_2^{-1} \cdot \alpha_1 \cdot p_1 = a \cdot b_0 \cdot \alpha_2^{-1} \cdot \eta$$

durch p_1^{m+1} teilbar, falls $a \cdot b$ es wäre; denn a ist ja durch p_1^m teilbar, also wäre in jedem der beiden Summanden p_1^{m+1} enthalten. Andererseits ist a nach Voraussetzung nur durch p_1^m, c nach dem letzten Resultat überhaupt nicht durch p_1 teilbar, und da $a \cdot c$ weniger wesentlich verschiedene Teiler enthält als $a \cdot b$ (weil nämlich alle Teiler von $a \cdot b_0$ in $a \cdot b$, nicht aber z. B. $a \cdot b$ in $a \cdot b_0$ enthalten ist), so war für $a \cdot c$ der zu beweisende Satz schon als gültig angenommen. Der hiermit erzielte Widerspruch erweist den Satz 4 als richtig.

Da für einen Ring von endlichem Grad, der nur zwei wesentlich verschiedene Primteiler p_1 und p_2 enthält*), sicher $p_1 + p_2 = \eta$ regulär ist, so folgt als Korollar des letzten Satzes:

Satz 5: *Ein Ring endlichen Grades, der nur zwei wesentlich verschiedene Primteiler enthält, ist stets zerlegbar.*

Bisher sind in diesem Paragraphen ausschließlich Ringe von endlichem Grade betrachtet und für sie die Existenz der Primteiler der Null und einige Eigenschaften derselben bewiesen worden. Offenbar sind die hierbei, besonders beim Existenzbeweis, benutzten Methoden auf *Ringe unendlich hohen Grades* nicht ausdehnbar; daß aber in Ringen der letzteren Art wirklich *Primteiler der Null überhaupt nicht notwendig existieren*, zeigt das folgende Beispiel:

Jedes Element A des zu betrachtenden Ringes $\mathfrak{R}$ sei ein Komplex von abzählbar unendlich vielen, in wohlgeordneter Reihe auftretenden reellen Zahlen a_i: $A = (a_1, a_2, a_3, \ldots)$; die Zahlen a_i können dabei beliebig gewählt werden, nur soll ihre Folge für jedes Element A periodisch sein, d. h. es soll zu A eine natürliche Zahl m (und also eine eindeutig bestimmte *kleinste* solche Zahl, die *Periodenlänge*) existieren derart, daß

$$A = (a_1, a_2 \ldots a_m, a_1, a_2, \ldots a_m, a_1, \ldots)$$

ist. Addition und Multiplikation seien definiert durch

$$(a_1, a_2, \ldots) + (b_1, b_2, \ldots) = (a_1 \overset{*}{+} b_1, a_2 \overset{*}{+} b_2, \ldots)$$
$$(a_1, a_2, \ldots) \cdot (b_1, b_2, \ldots) = (a_1 * b_1, a_2 * b_2, \ldots),$$

wobei $\overset{*}{+}$ und $*$ die Zeichen für die gewöhnliche Addition und Multiplikation der reellen Zahlen sind. Die Summe, die Differenz und das Produkt zweier Elemente mit den Periodenlängen m und n sind ersichtlich wieder Elemente aus $\mathfrak{R}$, deren Periodenlängen das kleinste gemeinsame Vielfache von m und n oder Teiler desselben sein werden. Alle Bedingungen R_1) bis R_{10}) und auch die Zerlegbarkeitsbedingung Z) sind erfüllt; Nullelement ist $(0, 0, 0, \ldots)$, Einheitselement $(1, 1, 1, \ldots)$. Nullteiler sind alle und nur die Elemente, in deren Periode wenigstens *eine* Null vorkommt; denn es ist z. B.

*) Ein Ring mit nur zwei Primteilern kann sehr wohl auch unendlich hohen Grad besitzen, da möglicherweise alle Potenzen eines Primteilers untereinander wesentlich verschieden sind (vgl. S. 23 ff.).

$$(a_1, \ldots a_{k-1}, 0, a_{k+1}, \ldots a_m, a_1, \ldots) \cdot (\overbrace{0, 0, \ldots 0}^{k-1 \text{ Glieder}}, \underbrace{1, \overbrace{0, \ldots 0}^{m-k \text{ Glieder}}, 0, \ldots}_{\text{Periode}}) = (0, 0, 0, \ldots).$$

Trotzdem enthält dieser Ring keinen Primteiler der Null; denn ist $A = (a_1, \ldots a_m, a_1, \ldots)$ ein ganz beliebiger Nullteiler, so ist

$$A = (\underbrace{a_1, a_2, \ldots a_m, \overbrace{1, 1, \ldots 1}^{m \text{ Glieder}}}_{\text{Periode}}, a_1, a_2, \ldots) \cdot (\underbrace{\overbrace{1, 1, \ldots 1}^{m \text{ Glieder}}, a_1, a_2, \ldots a_m}_{\text{Periode}}, 1, 1, \ldots),$$

und hier ist sowohl der erste wie auch der zweite Faktor wesentlich verschieden von A, d. h. A ist gewiß kein Primteiler.

Um daher auch bei Ringen unendlich hohen Grades das Vorhandensein von Primteilern der Null benutzen zu können, auf das sich alles Nachfolgende wesentlich stützen wird, und um zugleich die hier notwendigen unendlichen Prozesse vorwegzunehmen, setze ich für die weiter zu betrachtenden zerlegbaren Ringe *unendlich hohen Grades*, aber auch nur für diese, noch das Erfülltsein der folgenden Bedingung voraus:

$Z_{\infty})$ *In einem zerlegbaren Ring unendlich hohen Grades gibt es zu jedem vorgegebenen Nullteiler einen in ihm enthaltenen Primteiler der Null p, und für jeden solchen Primteiler läßt sich die Null darstellen in der Form $O = P \cdot \bar{P}$, wo $\bar{P}$ durch den Primteiler p nicht teilbar, P aber umgekehrt nur durch p und keinen von p wesentlich verschiedenen Primteiler teilbar ist.*

In einem solchen Ring ist dann möglicherweise ein Element darstellbar als Produkt einer Menge von Primteilern der Null, welche eine beliebig hohe transfinite Mächtigkeit besitzen kann; zur Veranschaulichung wird ein Beispiel eines derartigen Ringes am Schluß dieses Paragraphen gegeben werden.

Von nun an sollen in dieser Arbeit ausschließlich zerlegbare Ringe, die also den Bedingungen $R_{1})$ bis $R_{10})$ a. S. 9f. und $Z)$ a. S. 18 genügen, betrachtet werden; unter „Ring" schlechthin ist stets ein zerlegbarer zu verstehen, und zwar im Fall unendlich hohen Grades stets ein solcher zerlegbarer Ring, der auch noch der Bedingung $Z_{\infty})$ genügt.

p sei ein beliebiger Primteiler der Null im Ring $\mathfrak{R}$. Besitzt $\mathfrak{R}$ endlichen Grad, so können unter den Potenzen $p, p^2, p^3, \ldots$, die sämtlich Nullteiler sind, nicht unendlich viele wesentlich verschiedene sein; aber

auch bei Ringen unendlich hohen Grades kann und wird es häufig vorkommen, daß zwei dieser Potenzen einander äquivalent sind. Es sei p^n die niedrigste Potenz, die sich von einer früheren, etwa p^m $(m < n)$, nur unwesentlich unterscheide; da p^{n-1} wegen $m < n$ sicher durch p^m teilbar ist, so ist dann $p^n \backsim p^{n-1}$, d. h. $m = n - 1$. Ist $p^m = a \cdot p^{m+1}$, so ist auch $p^{m+m'} = a \cdot p^{m+m'+1}$ $(m' = 1, 2, \ldots)$, so daß folgt:

Satz 6: *Sind — was insbesondere bei Ringen endlichen Grades stets der Fall ist — die Potenzen $p, p^2, \ldots$ eines beliebigen Primteilers p im Ringe $\mathfrak{R}$ nicht sämtlich untereinander wesentlich verschieden, so gibt es eine natürliche Zahl m derart, daß die Potenzen $p, p^2, \ldots p^m$ alle untereinander wesentlich verschieden, alle folgenden Potenzen $p^{m+1}, p^{m+2}, \ldots$ aber sämtlich zueinander und zu p^m äquivalent sind.* Dies möge bezeichnet werden durch die Ausdrucksweise: Der Primteiler p steigt bis zum Exponenten m.

Es ist nun vor allem zu zeigen, daß es auch zerlegbare Ringe, also Ringe, die nicht nur die Bedingung Z), sondern auch Z_∞) erfüllen, von solcher Art gibt, daß sie Primteiler der Null p enthalten, für die *alle* Potenzen $p, p^2, p^3, \ldots$ untereinander wesentlich verschieden sind; ein solcher Ring ist dann sicher auch von unendlich hohem Grad. Auf Ringe dieser Art ist man meines Wissens bisher noch nirgends geführt worden; ihre Existenz ist aber auch aus folgender Erwägung heraus merkwürdig: Ist p ein Primteiler der Null, dessen Potenzen sämtlich untereinander wesentlich verschieden sind, und P ein nach Z_∞) existierender Nullteiler von der Art, daß $P \cdot \bar{P} = O$ ist, wo P, aber nicht $\bar{P}$ durch den Primteiler p teilbar ist, so kann man wiederum nach der beim Beweis des Satzes 2 auf S. 16 eingeschlagenen Methode eine Zerlegung $P = p \cdot P'$ finden, für die P und P' wesentlich verschieden sind; da hier offenbar P' durch *jede* Potenz p^m von p teilbar ist, liegt es nahe, nach Analogie mengentheoretischer Sätze zu erwarten, daß P' auch durch $p \cdot P' = P$ teilbar sein müsse, womit die Nichtexistenz derartiger Ringe erwiesen wäre. Der innere Grund des Unterschieds liegt darin, daß das Analogon zum Axiom der Vereinigungsmenge der Mengenlehre, das die Existenz eines kleinsten gemeinsamen Vielfachen gegebener Nullteiler sichern würde, hier nicht existiert.

Um nun einen Ring von der gewünschten Eigenschaft zu bilden und anschaulich zu machen, gehe ich von einem geometrischen Bild aus. Man denke sich den Punkten einer Strecke von der Länge 2 die Werte

von -1 bis $+1$ als Abszissen zugeordnet und markiere unter ihnen besonders die Punkte mit den Abszissen $\pm 1, \pm\frac{1}{2}, \pm\frac{1}{4}, \ldots \pm\frac{1}{2^\nu}, \ldots$; ferner bezeichne man den Punkt von der Abszisse -1 mit E oder p^0, den Punkt $-\frac{1}{2}$ mit p, den Punkt $-\frac{1}{4}$ mit $p^2, \ldots$ den Punkt $-\frac{1}{2^\nu}$ mit p^ν, andererseits den Punkt $+1$ mit N oder $\frac{N}{p^0}$, den Punkt $+\frac{1}{2}$ mit $\frac{N}{p}$, den Punkt $+\frac{1}{4}$ mit $\frac{N}{p^2}, \ldots$ den Punkt $+\frac{1}{2^\nu}$ mit $\frac{N}{p^\nu}$. Schließlich definiere man zwischen diesen Punkten oder Symbolen eine Multiplikation durch die Festsetzungen

$$p^\mu \cdot p^\nu = p^{\mu+\nu},\quad \frac{N}{p^\mu}\cdot\frac{N}{p^\nu} = N,\quad \frac{N}{p^\mu}\cdot p^\nu = p^\nu \cdot \frac{N}{p^\mu} = \frac{N}{p^{\mu-\nu}} \text{ für } \mu > \nu,$$

$$\frac{N}{p^\mu}\cdot p^\nu = p^\nu \cdot \frac{N}{p^\mu} = N \text{ für } \mu \leqq \nu.$$

Diese Formeln besagen, es solle, je nachdem der Multiplikator von der Form p^ν oder von der Form $\frac{N}{p^\nu}$ ist, vom Multiplikanden aus um ν oder um unendlich viele Punkte nach der positiven Richtung fortgeschritten werden, mit der Maßgabe, daß die Multiplikation kommutativ ist und der Punkt N nicht überschritten werden darf.

Man betrachte nun E als das universale Einheitselement und N als das Nullelement eines Ringes $\mathfrak{R}$, in dem alle natürlichen Multipla von E untereinander verschieden und regulär seien, und der alle Symbole der Form $\frac{\alpha_1 \cdot P_1 + \alpha_2 \cdot P_2 + \cdots + \alpha_m \cdot P_m}{\beta_0 + \beta_1 \cdot Q_1 + \beta_2 \cdot Q_2 + \cdots + \beta_n \cdot Q_n}$ als Elemente enthalte, wobei die α_i und β_i beliebige rationale Multipla von E mit der einzigen Beschränkung $\beta_0 \neq N$, die P_i und Q_i aber beliebige Elemente der Doppelreihe $E, p, p^2, p^3, \ldots N, \frac{N}{p}, \frac{N}{p^2}, \frac{N}{p^3}, \ldots$ seien. Gleichheit, Addition und Multiplikation mögen formal ganz wie bei rationalen Funktionen erklärt werden, nur daß Produkte der P_i und Q_i nach den vorher gegebenen Regeln zu bilden sind. Dann sind offenbar alle Bedingungen $R_{1)}$ bis $R_{10)}$, $Z)$ und $Z_{\infty)}$ erfüllt; Nullteiler sind alle und nur die Elemente, in deren „Zähler“ (nach Zusammenfassung gleichartiger Glieder) alle P_i von E verschieden sind. Primteiler der Null insbesondere die zu p äquivalenten Elemente, und da der Ring also nicht zwei wesentlich verschiedene Primteiler enthält, wird $Z_{\infty)}$ durch $P = N,\ P \backsim E$ erfüllt. In diesem Ring sind alle Potenzen von p untereinander wesentlich verschieden und hat z. B. jeder Nullteiler der Form $\frac{N}{p^\nu}$ $(\nu > 0)$ die Eigenschaft, zwar durch alle Potenzen

$p, p^2, p^3, \ldots$ des Primteilers p teilbar zu sein, aber sich wesentlich zu ändern bei der Multiplikation mit p.

Um daher die Untersuchung im folgenden ganz allgemein führen zu können, will ich auch für einen Ring, in dem *alle* Potenzen $p, p^2, \ldots$ untereinander wesentlich verschieden sind, eine Bezeichnung analog der im anderen Fall verwendeten einführen. Es sei nämlich in einem solchen Ring, der natürlich stets von unendlich hohem Grad ist, $O = P \cdot \bar{P}$ eine Zerlegung der Null im Sinn von $Z_{\infty)}$, bei welcher P den Primteiler p enthält. Dann ist auch $P \cdot p$ in O und daher, weil $\bar{P}$ durch p nicht teilbar ist, in P enthalten, d. h. es ist $P \backsim P \cdot p \backsim P \cdot p^2 \backsim \cdots$; P spielt offenbar für den Primteiler p genau die nämliche Rolle wie vorher p^m. Ich will daher auch in diesem Fall, wo alle Potenzen von p untereinander wesentlich verschieden sind, den gemäß $Z_{\infty)}$ bis auf äquivalente Elemente eindeutig bestimmten, allein durch den Primteiler p teilbaren Nullteiler P als eine symbolische Potenz p^m schreiben und m den Exponenten nennen, bis zu dem p steigt; m ist aber in diesem Fall lediglich als ein Symbol zu betrachten, das nur durch die Festsetzung $p^m = P$ definiert ist (und das man etwa, wenn man will, identifizieren kann mit der Ordinalzahl der Menge aller wesentlich verschiedenen Teiler von P, falls diese so angeordnet ist, daß jedes folgende Element in ihr durch jedes voraufgehende teilbar ist; also im Fall des letzten Beispiels $m = \omega + {}^*\omega$).

In den beiden Fällen eines endlichen und eines symbolischen m nenne ich den bis auf äquivalente Elemente eindeutig bestimmten Nullteiler $P = p^m$ einen zum Primteiler p gehörigen primären Teiler der Null oder kurz Primärteiler. Steigt ein Primteiler nur bis zum Exponenten 1, so ist er zugleich Primärteiler. Dann und nur dann ist die Null selbst Primärteiler (und zwar dann der einzige), wenn der Ring nicht zwei wesentlich verschiedene Primteiler enthält. Die Primärteiler können auch charakterisiert werden als Nullteiler, die nur einen einzigen Primteiler enthalten und sich nur unwesentlich ändern, wenn man sie mit beliebigen ihrer Teiler multipliziert.

Beispiel für R_{360}: Der Primteiler 2 steigt in R_{360} bis zum Exponenten 3, der Primteiler 3 bis zum Exponenten 2, der Primteiler 5 bis zum Exponenten 1; z. B. sind 2, 4, 8 wesentlich verschieden, aber es ist $8 \backsim 16$ wegen $16 = 2 \cdot 8$, $8 = 23 \cdot 16$.

Die Primärteiler von R_{360} sind: 8, 16, 32, 56, 64, 88, ...; 9, 27, 63, 81, 99, ...: 5, 25, 35, 55, 65, ..., und zwar gehören diejenigen der ersten Reihe zum Primteiler 2, die der zweiten zu 3, die der dritten zu 5 und die Primärteiler jeder Reihe sind untereinander äquivalent. — Dagegen steigen z. B. in Ringen g-adischer Zahlen alle Primteiler bis zum Exponenten 1.

Offenbar gilt:

Satz 7: *Ein Ring, dessen sämtliche Primteiler nur bis zu endlichen Exponenten steigen, ist dann und nur dann von unendlich hohem Grad, wenn er unendlich viele wesentlich verschiedene Primteiler enthält.*

Nunmehr sind alle Materialien zum Beweis des Fundamentalsatzes über die eindeutige Zerlegung vollständig entwickelt:

Satz 8: *In einem (zerlegbaren) Ring ist die Zerlegung eines beliebigen Nullteilers, insbesondere also der Null selbst, in Primteiler der Null bis auf reguläre Faktoren eindeutig, wenn man äquivalente Nullteiler nicht als verschieden betrachtet.*

Was zunächst den *Sinn* dieses Satzes betrifft, auf den etwas näher einzugehen erforderlich ist, so ist er für Ringe endlichen Grades klar, ebenso auch in Ringen von unendlich hohem Grad in bezug auf diejenigen Primteiler, die in dem zu untersuchenden Nullteiler nur in einer bestimmten endlichen Potenz enthalten sind; nur das eine ist — bei allen Ringen endlichen Grades wie auch in Ringen unendlich hohen Grades bei solchen Primteilern p, die nur bis zu endlichen Exponenten steigen — zu beachten, daß in irgend zwei Zerlegungen des zu untersuchenden Nullteilers die Anzahlen α und β, in denen ein Primteiler p einschließlich der ihm äquivalenten beiderseits vorkommt, natürlich nur dann übereinzustimmen brauchen, wenn α oder β kleiner ist als der Exponent m, bis zu dem der Primteiler p steigt; denn ist $\alpha \geqq m$ und $\beta \geqq m$, so ist ja nach der Definition von m *stets* $p^{\alpha} \backsim p^{\beta}$. (Z. B. ist so in R_{360}: $32 = 2^5 = 23 \cdot 2^6$.) Bei Ringen unendlich hohen Grades aber, wo eine nicht allgemein als definiert vorauszusetzende Zerlegung in unendlich viele Faktoren in Frage kommen kann, ist die Behauptung des Satzes diese: Sind irgend zwei Zerlegungen eines Nullteilers A in je endlich viele Faktoren gegeben, und ist ein Primteiler p in einem Faktor der einen Zerlegung enthalten, so ist auch mindestens ein Faktor der andern durch p teilbar; sind insbesondere die in den Zerlegungen von A enthaltenen zu p äquivalenten Elemente zu je einem, P bzw. P', zusammengefaßt, so daß $A = P \cdot \bar{P} = P' \cdot \bar{P'}$

ist, wobei $\bar{P}$ und $\bar{P'}$ nicht durch p, P und P' aber nur durch p und keinen davon wesentlich verschiedenen Primteiler teilbar sind, so ist stets $P \frown P'$.

Der Beweis des Satzes ist nunmehr ganz trivial. Es seien nämlich

$$A = a_1 \cdot a_2 \cdots a_m = b_1 \cdot b_2 \cdots b_n$$

irgend zwei Zerlegungen von A in endlichviele Faktoren, und auf der linken Seite sei der Primteiler p in einem der a_i enthalten. Da ein Primteiler nur Nullteiler enthält, die ihm selbst äquivalent sind, so folgt aus der Zerlegbarkeitsbedingung Z) durch sukzessive Anwendung, daß, falls keiner der Faktoren b_i den Primteiler p enthielte, auch A nicht durch p teilbar wäre; da dies der Voraussetzung widerspricht, ist der erste Teil des Satzes bewiesen. Ferner seien jetzt wie zu Ende des vorigen Absatzes P und P' die beiderseits aus allen und nur den zu p äquivalenten Nullteilern zusammengesetzten Elemente, so daß $A = P \cdot \bar{P} = P' \cdot \bar{P'}$ ist; steigt p nur bis zu einem endlichen Exponenten oder ist p nur in endlicher Potenz in A enthalten, so läßt sich die Zerlegung von A durch Umstellung der Faktoren nach Satz 3 des § 1 auf S. 11 offenbar immer auf diese Form bringen. Dann ist P in $P' \cdot \bar{P'}$ und also, da $\bar{P'}$ den Primteiler p nicht enthält, nach Z) in P' enthalten, ebenso aber auch umgekehrt P' in P, d. h. es ist $P \frown P'$, w. z. b. w..

Zum Abschluß dieses Paragraphen soll als Beispiel ein Ring $\mathfrak{R}$ angegeben werden, für den *die Menge aller wesentlich verschiedenen Primteiler der Null nicht nur unendlich, sondern sogar von der Mächtigkeit des Kontinuums ist.* Die Elemente von $\mathfrak{R}$ seien Einheitsstrecken einschließlich ihrer Enden, deren Punkte einander umkehrbar eindeutig und (etwa in der Richtung von links nach rechts) ähnlich zugeordnet seien. Von der durch jede Einheitsstrecke gebildeten Punktmenge sei eine völlig willkürliche Teilmenge von Punkten besonders markiert, etwa durch Bezeichnung der Punkte mit je einer 0; zur Unterscheidung werde allen Punkten jeder Einheitsstrecke, die nicht in dieser Weise markiert sind, eine 1 beigeschrieben, und der Kürze wegen schlechthin von Punkten 0 und Punkten 1 gesprochen. Der Ring $\mathfrak{R}$ werde nun gebildet von allen Einheitsstrecken mit *allen möglichen* verschiedenen solchen Markierungen, er entsteht also durch Belegung einer kontinuierlichen Menge mit den Symbolen 0, 1; unter den Elementen von $\mathfrak{R}$ befindet sich demnach auch die Strecke N, deren Punkte sämtlich mit 0 markiert sind, und die

Strecke E, die lauter Punkte 1 enthält. Die Summe, die Differenz und das Produkt zweier Strecken sollen dadurch entstehen, daß je zwei einander in der eingangs erwähnten Art zugeordnete Punkte auf die sogleich zu definierende Weise addiert, subtrahiert und multipliziert werden und als Summe, Differenz und Produkt die durch die entstehenden Markierungen gekennzeichneten Strecken betrachtet werden. Für einander entsprechende Punkte gelten Operationsregeln wie in der gewöhnlichen Arithmetik, nur daß die Addition modulo 2 genommen wird, also:

$$1 + 1 = 0 + 0 = 0,\ 1 + 0 = 0 + 1 = 1;$$
$$1 \cdot 1 = 1;\ 1 \cdot 0 = 0 \cdot 1 = 0 \cdot 0 = 0.$$

Hiernach ist N das Nullelement, E das Einheitselement von $\mathfrak{R}$ und für jede Strecke A ist stets $A = -A$. Nullteiler sind alle und nur die Strecken, die *wenigstens einen* Punkt 0 enthalten; denn ist für eine solche Strecke A M die Menge aller Punkte 0, so steht jede Strecke B, bei der mindestens die Komplementärmenge von M ausschließlich aus Punkten 0 besteht, zu A in der Beziehung $A \cdot B = N$. Primteiler der Null sind alle und nur die Strecken, die *genau einen* Punkt 0 enthalten; sie sind gleichzeitig die Primärteiler des Ringes, da offenbar jeder Primteiler hier nur bis zum Exponenten 1 steigt. Jede Strecke von $\mathfrak{R}$ ist ersichtlich eindeutig als Produkt von endlich oder auch — wenn man in einleuchtender Weise die hier vorkommenden harmlosen unendlichen Produkte zuläßt — unendlich vielen solchen Primteilern darstellbar.

§ 3. Die normierten Primärteiler und die normalen Primteiler.

Unter allen zu einem Primteiler p oder zu einem Primärteiler P eines Ringes äquivalenten Elementen war in der bisherigen Betrachtung keines vor einem anderen ausgezeichnet; diese Gleichberechtigung soll jetzt zerstört und damit die Struktur eines Ringes noch anschaulicher übersehbar gemacht werden.

Zunächst sei P' ein zum Primteiler p gehöriger Primärteiler und $P' \cdot \overline{P'} = O$, wo $\overline{P'}$ durch p nicht teilbar sei. Nach einer auf S. 25 unten gemachten Bemerkung ist dann $P' \cdot P'$ ein zu P' äquivalenter Primärteiler, der vermöge

$$P' \cdot P' = P' \cdot P' + P' \cdot P' = P' \cdot (P' + P')$$

sich in der Form $P' \cdot P' = P' \cdot \alpha$ darstellt, wo $\alpha = P' + \overline{P'}$ regulär ist; denn α

kann weder durch p (wegen $P' = \alpha - P'$) noch durch einen von p wesentlich verschiedenen, also in P' enthaltenen Primteiler (wegen $P' = \alpha - P'$) teilbar sein. Setzt man $P' \cdot \alpha^{-1} = P$, so folgt $P' \cdot P = P' \cdot \varepsilon = P'$; ich will zeigen, daß der zu P' äquivalente Primärteiler P durch besondere, von der Wahl von P' unabhängige Eigenschaften ausgezeichnet ist.

$P'' = a \cdot P' \cdot b$ sei ein beliebiges zu P' äquivalentes Element; dann läßt sich mittels Anwendung von $R_{9)}$ und eventuell des oben benutzten Verfahrens der Addition von $O = P' \cdot \overline{P'}$ offenbar P'' auf jede der Formen $P' \cdot \beta$ oder $\gamma \cdot P'$ bringen, wo β und γ regulär sind. Zunächst folgt dann, wenn P wieder das im vorigen Absatz definierte Element bedeutet, $\gamma \cdot P' \cdot P = \gamma \cdot P'$, also $P'' \cdot P = P''$, d. h. P spielt in bezug auf die zu P' äquivalenten Elemente die Rolle eines rechtshändigen Einheitselements; ferner ist

$$P' \cdot \beta \cdot \beta^{-1} \cdot \alpha^{-1} \cdot P = P \text{ oder } P'' \cdot (\beta^{-1} \cdot \alpha^{-1} \cdot P) = P,$$

d. h. der zu P' äquivalente Primärteiler $\beta^{-1} \cdot \alpha^{-1} \cdot P$ ist zu P'' reziprok in bezug auf P als Einheitselement. Da auch das Produkt zweier zu P' äquivalenter Primärteiler wieder ein solcher ist, so bilden alle diese äquivalenten Elemente nach der Definition auf S. 8 in bezug auf die Multiplikation eine Gruppe. Ist ferner A ein *beliebiges* durch P teilbares Element: $A = a \cdot P$, so ist offenbar auch $A \cdot P = A$. Setzt man noch fest:

Definition 1: Jedes Ringelement a, das der Beziehung $a \cdot a = a$ genügt, soll als normiert bezeichnet werden, so hat man:

Satz 1: *Alle zu irgendeinem primären Nullteiler äquivalenten Elemente bilden in bezug auf die Multiplikation eine Gruppe, es gibt also unter ihnen insbesondere ein einziges normiertes Element P, den zum Primteiler p gehörigen normierten Primärteiler, der das neutrale Element der Gruppe ist. Jeder normierte Primärteiler ist allgemeiner auch ein Einheitselement für alle durch ihn teilbaren Elemente. Sind A, B, C irgend drei zu P äquivalente Primärteiler, so folgt aus $A \cdot B = A \cdot C$ stets $B = C$ und die Gleichungen $A \cdot X = B$ bzw. $Y \cdot A = B$ haben je eine einzige Lösung X bzw. Y unter den zu P äquivalenten Elementen.*

Die letzten Behauptungen dieses Satzes folgen einfach aus der Gruppeneigenschaft; ist z. B. $A = P \cdot \alpha$, $B = P \cdot \beta$, so ist $X = \alpha^{-1} \cdot P \cdot \beta$ die zu P äquivalente Lösung der Gleichung $A \cdot X = B$, welche natürlich auch noch andere, aber von P wesentlich verschiedene Lösungen besitzt.

Beispiel für R_{360}: Die normierten Primärteiler sind hier die folgenden: 136, 81, 145.

Mittels der letzten Ergebnisse ist es leicht, den folgenden Satz abzuleiten, der eine teilweise Umkehrung des Satzes 4 von § 2 auf S. 18 darstellt:

Satz 2: *Notwendige Bedingung für die Zerlegbarkeit eines kommutativen Ringes* $\mathfrak{R}$ *ist, daß die Summe irgend zweier wesentlich verschiedener normierter Primärteiler der Null stets ein reguläres Element darstellt; nur dann braucht diese Bedingung nicht erfüllt zu sein, wenn das Element* $\varepsilon + \varepsilon$ *aus* $\mathfrak{R}$ *ein Nullteiler ist.*

Zum Verständnis dieses Satzes ist zu bemerken, daß bei der Definition und dem Existenzbeweis der Primärteiler in Ringen endlichen Grades die Zerlegbarkeit nicht benutzt worden ist; bei Ringen unendlich hohen Grades ist natürlich die Bedingung $Z_{\infty)}$ als erfüllt vorauszusetzen, da mittels ihrer die Primärteiler erst definiert wurden.

Beispiel für den Ring der Kongruenzklassen modulo 315: Hier sind 36, 190, 91 die normierten Primärteiler und es ist:

$36 + 190 = 226$ (regulär), $36 + 91 = 127$ (regulär), $91 + 190 = 281$ (regulär).

Beweis: $\mathfrak{R}$ sei ein zerlegbarer Ring, in dem die Multiplikation kommutativ und das Element $\varepsilon + \varepsilon = 2\varepsilon$ regulär sei. Zunächst kann dann die Summe zweier verschiedener normierter Primärteiler $P = p^m$ und $Q = q^n$ weder p noch q enthalten. Enthält $\mathfrak{R}$ überhaupt nur zwei wesentlich verschiedene Primteiler, so ist daher der Satz richtig. Im anderen Fall ist:

$$(p^m + q^n) \cdot (p^m + q^n) = p^m \cdot p^m + q^n \cdot q^n + 2\,(p^m \cdot q^n)$$

oder, da p^m und q^n normiert sind:

$$(p^m + q^n) \cdot (p^m + q^n - \varepsilon) = 2\varepsilon \cdot p^m \cdot q^n.$$

Enthielte nun $p^m + q^n$ einen von p und q wesentlich verschiedenen Primteiler, so müßte dieser auch in $2\varepsilon \cdot p^m \cdot q^n$ enthalten sein, was ausgeschlossen ist, da $\mathfrak{R}$ zerlegbar und 2ε regulär sein sollte; Satz 2 ist also als richtig erwiesen.

Daß aber die für den Fall, wo 2ε ein Nullteiler ist, ausgesprochene Ausnahme nicht etwa auf der Besonderheit des Beweisverfahrens beruht, vielmehr in der Art der Bedingung notwendig gelegen ist, zeigt z. B. jeder Ring von Kongruenzklassen für eine beliebige natürliche gerade Zahl g als Modul, die nur außer 2 noch mindestens zwei weitere gewöhnliche Primzahlen enthält. Offenbar gehört nämlich zu jeder in g enthaltenen Primzahl eine Serie

äquivalenter Primteiler der Null und umgekehrt; 2 und die äquivalenten Klassen bilden eine solche, zum Faktor 2 gehörige Serie, während alle anderen Primteiler wie auch ihre zugehörigen Primärteiler ungerade sind. Der Ring ist kommutativ und zerlegbar; trotzdem ist offenbar die Summe aus irgend zwei beliebigen (insbesondere also auch normierten) Primärteilern, die zu verschiedenen ungeraden Primfaktoren von g gehören, stets durch den Primteiler 2 teilbar. Z. B. sind 81 und 145 die zu 3 und 5 gehörigen normierten Primärteiler von R_{360} und es ist $81+145=226$ äquivalent dem Primteiler 2.

Ist ein Primteiler der Null in einem Ring $\mathfrak{R}$ zugleich Primärteiler, so kann man ihn nach dem vorher angegebenen Verfahren normieren und dann von einem normierten Primteiler sprechen. Vergleicht man alsdann den Satz 4 des § 2 auf S. 18 und den hier soeben bewiesenen Satz, so ergibt sich:

Satz 3: *Ein kommutativer Ring von endlichem Grad, dessen Primteiler sämtlich nur bis zum Exponenten* 1 *steigen und in dem* $\varepsilon+\varepsilon$ *ein reguläres Element ist, ist dann und nur dann zerlegbar, wenn die Summe irgend zweier verschiedener normierter Primteiler stets regulär ist.*

Solche Ringe sind z. B. jeder Ring von Kongruenzklassen für eine beliebige ungerade, kein Quadrat enthaltende zusammengesetzte Zahl als Modul oder jeder Ring rationaler g-adischer Zahlen, wobei g eine beliebige, wenigstens zwei verschiedene Primzahlen enthaltende natürliche Zahl bedeutet.

Nachdem jetzt in jeder Serie äquivalenter *Primärteiler* ein besonderer ausgezeichnet worden ist, soll Ähnliches für äquivalente *Primteiler* angestrebt werden; hierbei muß offenbar ein anderer Weg eingeschlagen werden, da ein Primteiler, der nicht schon selbst Primärteiler ist, durch Multiplikation mit sich selbst oder einem äquivalenten Primteiler in ein wesentlich verschiedenes Element übergeht, also gewiß nicht normiert sein kann. Ich beginne mit der

Definition 2: Ist P' ein beliebiger Primärteiler aus $\mathfrak{R}$, so heißt ein Element A aus $\mathfrak{R}$ normal in bezug auf P' oder kurz normal, wenn es die Beziehung $P' \cdot A = P'$ erfüllt, also für P' ein rechtshändiges Einheitselement darstellt. Es gilt:

Satz 4: *Alle in bezug auf den Primärteiler* P' *normalen Ringele-*

mente sind Teiler von P' und die Produkte irgendwelcher unter ihnen sind wieder normal in bezug auf P'. Zu jedem normalen Element aus $\mathfrak{R}$, das kein Primärteiler ist, gibt es — außer eventuell in dem Fall, daß 2ε ein Nullteiler in $\mathfrak{R}$ ist — mindestens ein weiteres ihm äquivalentes, das gleichfalls normal ist, und, wenn die natürlichen Vielfachen des Einheitselements von $\mathfrak{R}$ sämtlich regulär sind, sogar unendlichviele verschiedene äquivalente normale Elemente.

Die ersten Behauptungen folgen unmittelbar aus der Definition der normalen Elemente. Was den zweiten Teil des Satzes betrifft, der übrigens hier weiterhin nicht mehr benutzt wird, und dessen Beweis daher nur skizziert werde, so sei $P \cdot \bar{P} = O$, wo $\bar{P}$ den Primteiler p, zu dem der Primärteiler P gehört, nicht mehr enthalte; ist dann $P \cdot A = P$, so ist auch $P \cdot B = P$, wo $B = A \cdot (\varepsilon + \bar{P})$, und hier ist erstens, wenn A keinen Primärteiler darstellt, $A \cdot \bar{P}$ nicht durch P teilbar und also $B \neq A$, zweitens kann $\bar{P}$ als so gewählt vorausgesetzt werden, daß unter der Annahme der Regularität von 2ε nach Analogie der beim Beweis des Satzes 2 benutzten Methode das Element $\varepsilon + \bar{P}$ leicht als regulär, also A und B als äquivalent zu erweisen sind. Sind schließlich alle natürlichen Vielfachen von ε regulär, so sind auch alle Elemente der Form $A \cdot (\varepsilon + m\bar{P})$, wo $\bar{P}$ wie vorhin gewählt ist und m jede beliebige natürliche Zahl darstellt, normal, untereinander verschieden und zu A äquivalent, w. z. b. w..

Sind hiernach die normalen Elemente, deren Existenz übrigens erst noch nachzuweisen sein wird, auch allerdings nicht wie die normierten durch eindeutige Bestimmtheit unter allen äquivalenten Elementen ausgezeichnet, so hat man in ihnen doch, wie durch Umkehrung der letzten Betrachtungen oder auch an Hand von Beispielen (vgl. nächste Seite) zu erkennen ist, sehr spezielle Vertreter je einer Klasse äquivalenter Nullteiler, und ihre Eigenschaften können, wie jetzt zu zeigen ist, zur Charakterisierung besonderer *Primteiler* mit Vorteil benutzt werden. Dabei sei noch im voraus bemerkt, daß in Ringen, deren Primteiler sämtlich äquivalent sind, die Null der einzige Primärteiler ist, also alle Elemente normal sind und somit die Betrachtung jede Bedeutung verliert.

Es sei jetzt p' ein beliebiger Primteiler aus $\mathfrak{R}$, P ein zu p' gehöriger Primärteiler und $P \cdot \bar{P} = O$, wo $\bar{P}$ durch p' nicht teilbar sei. Dann ist

$$P \cdot p' = P \cdot (p' + \bar{P}) = P \cdot \alpha,$$

wo α regulär ist; setzt man also $p' \cdot \alpha^{-1} = p$, so ist $P \cdot p = P$, d. h. p ist normal in bezug auf P. Wie beim Beweis des Satzes 1 (S. 29) erkennt man, daß p auch normal ist in bezug auf die zu P äquivalenten Primärteiler, ferner kann man, genau wie dies für Primteiler soeben geschah, aus *jedem* Teiler von P einen äquivalenten normalen bilden. Da schließlich nach Satz 4 zugleich mit p auch $p^2, p^3, p^4, \ldots$ normal sind, so hat man:

Satz 5: *Ist p' ein beliebiger Primteiler, P ein zu p' gehöriger Primärteiler eines Ringes $\mathfrak{R}$, so gibt es unter den zu p' äquivalenten Elementen mindestens einen normalen Primteiler p, der für alle zu ihm gehörigen Primärteiler und allgemeiner für alle durch letztere teilbaren Ringelemente ein rechtshändiges Einheitselement darstellt. Allgemein gibt es in jeder Klasse aller zu einem gegebenen Teiler von P äquivalenten Elemente je mindestens ein normales Element von den nämlichen Eigenschaften, und zwar sind $\varepsilon, p, p^2, p^3, \ldots$ solche Elemente in den durch sie gekennzeichneten Klassen. Normale Primärteiler und normierte Primärteiler sind identische Begriffe; steigt insbesondere der Primteiler p' nur bis zum endlichen Exponenten m, so ist der zu ihm gehörige normierte Primärteiler genau die m-te Potenz jedes in bezug auf ihn normalen Primteilers p.*

Beispiel für R_{360}: Die normalen Primteiler von R_{360} sind (vgl. dagegen die Aufzählung *aller* Primteiler a. S. 15): 46, 226; 201, 321; 145. Dabei ist $46 \backsim 226 \backsim 2$, $201 \backsim 321 \backsim 3$, während $145 \backsim 5$ und als normierter Primärteiler eindeutig bestimmt ist. Ferner ist z. B. $46^2 = 316$ wieder normal, während $46^3 = 136 = 46^4 = \cdots$ der zu 2 gehörige normierte Primärteiler ist; ebenso ist $201^2 = 81 = 201^3 = \cdots$.

Zum Schluß sei noch ein bemerkenswerter allgemeiner, bisher nur in speziellen Fällen bewiesener und benutzter Satz angeführt, der die Umkehrung des Satzes 4 von § 1 auf S. 13 darstellt:

Satz 6: *Irgend zwei äquivalente Elemente eines zerlegbaren Ringes können durch Multiplikation mit je einem regulären Element ineinander übergeführt werden.*

Dieser scheinbar selbstverständliche Satz bedarf hier im Gegensatz zur gewöhnlichen Arithmetik eines eingehenden Beweises, da trotz $A \backsim B$ sehr wohl $A = a \cdot B$, $B = b \cdot A$ sein kann, wo a und b Nullteiler sind. (Z. B. ist in R_{360}: $16 = 2 \cdot 8$, $8 = 68 \cdot 16$.) Doch sind die Materialien zum Beweis jetzt völlig entwickelt, so daß es genügt, dessen Gang anzudeuten. Man erkennt nämlich leicht, daß die Faktoren a und b nur solche *Primteiler* enthalten können, deren zugehörige Primärteiler in A und B ent-

halten sind. Durch eventuelle multiplikative Hinzufügung weiterer normaler Nullteiler dieser Art oder, falls A und B unendlichviele wesentlich verschiedene Primteiler enthalten sollten, durch Hinzufügung eines geeigneten normierten Nullteilers zu den schon in a und b enthaltenen und durch darauffolgende Addition einer geeigneten Darstellung der Null, wie dies bei den Beweisen der Sätze 1 und 5 (S. 28 und 32) geschah, lassen sich dann a und b in reguläre Elemente verwandeln, wie gewünscht.

Faßt man die wesentlichsten Ergebnisse dieses und des vorigen Paragraphen für Ringe endlichen Grades in anschaulicher Form zusammen, so erhält man folgendes

Schlußergebnis: *$\mathfrak{R}$ sei ein zerlegbarer Ring endlichen Grades und $(p_1, p_2, \dots p_n)$ ein vollständiges System wesentlich verschiedener normaler Primteiler aus $\mathfrak{R}$; dann gibt es zu jedem p_i einen Exponenten m_i, bis zu dem p_i steigt. Man bilde dann erstens das System aller regulären Elemente aus $\mathfrak{R}$, das in bezug auf die Multiplikation eine Gruppe bildet, und ferner die n Paenegruppen (gleichfalls in bezug auf die Multiplikation verstanden)*

$$(\varepsilon, p_1, p_1^2, \dots p_1^{m_1});\ (\varepsilon, p_2, p_2^2, \dots p_2^{m_2});\ \dots (\varepsilon, p_n, p_n^2, \dots p_n^{m_n}).$$

Dann hat die Reihe dieser $n+1$ Systeme folgende Eigenschaften:

1. *Kein Element aus $\mathfrak{R}$, außer dem in jedem System vorkommenden Einheitselement, ist zugleich in zwei Systemen enthalten.*

2. *Unter den Nullteilern dieser Systeme gibt es keine zwei äquivalenten.*

3. *Jedes Element aus $\mathfrak{R}$ ist — bis auf die Reihenfolge und eine durch deren Veränderung bedingte Modifikation des regulären Faktors — auf eine einzige Weise als Produkt aus je einem Element jedes dieser Systeme darstellbar.*

§ 4. Die Orthogonalteiler. Die Zerlegung der Ringe.

War bisher fast ausschließlich die multiplikative Zerlegung der Ringelemente Gegenstand der Betrachtung, so soll in diesem Paragraphen die Addition in den Vordergrund treten und der Ring in gewisser Weise additiv zerlegt werden.

Definition 1: Ist $P \cdot \bar{P} = O$, wo P ein zum Primteiler p aus $\mathfrak{R}$ gehöriger Primärteiler ist, während $\bar{P}$ den Primteiler p nicht mehr enthält, so heiße P ein dem Primteiler p komplementärer orthogonaler Teiler der Null oder kurz Orthogonalteiler.

Offenbar sind zwei zu wesentlich verschiedenen Primteilern komplementäre Orthogonalteiler auch untereinander wesentlich verschieden und umgekehrt. Der Fall, daß alle Primteiler des betrachteten Ringes untereinander äquivalent sind, führt ersichtlich zu Trivialitäten und soll von nun an stets ausgeschlossen bleiben; enthält der Ring nur zwei wesentlich verschiedene Primteiler, so sind die zum einen gehörigen Primärteiler zugleich die dem anderen komplementären Orthogonalteiler.

Die Orthogonalteiler von R_{360} sind so: 72, 144, 216, 288 (komplementär zum Primteiler 5); 40, 80, 160, 200, 280, 320 (komplementär zu 3); 45, 135, 225, 315 (komplementär zu 2).

Satz 1: *Das Produkt irgend zweier wesentlich verschiedener Orthogonalteiler aus* $\mathfrak{R}$ *ist stets gleich Null.*

p und q seien nämlich zwei wesentlich verschiedene Primteiler aus $\mathfrak{R}$, $\bar{P}$ und $\bar{Q}$ zwei ihnen komplementäre Orthogonalteiler, und es sei $P \cdot \bar{P} = Q \cdot \bar{Q} = O$, wo P und Q Primärteiler bedeuten. Da Q (abgesehen von regulären Elementen) keinen Teiler besitzt, der auch in P enthalten ist, so muß $\bar{P}$ durch Q teilbar sein, d. h. $Q \cdot \bar{Q}$ ist in $\bar{P} \cdot \bar{Q}$ enthalten, oder es ist $\bar{P} \cdot \bar{Q} = O$, w. z. b. w..

Da jeder dem Primteiler p komplementäre Orthogonalteiler $\bar{P}'$ durch alle und nur die von p wesentlich verschiedenen Primteiler teilbar ist, so ist $\bar{P}' \cdot \bar{P}' \backsim \bar{P}'$, und zwar, wie man analog dem Verfahren von S. 28 unten erkennt oder aus Satz 6 des § 3 auf S. 33 folgert, $\bar{P}' \cdot \bar{P}' = \bar{P}' \cdot \alpha$, wo α regulär ist. Setzt man $\bar{P}' \cdot \alpha^{-1} = \bar{P}$, so folgt also: $\bar{P}' \cdot \bar{P} = \bar{P}'$. Überlegungen analog jenen, die auf S. 29 zum Satz 1 des § 3 führten, ergeben daher den

Satz 2: *Alle zu irgendeinem orthogonalen Nullteiler äquivalenten Elemente bilden in bezug auf die Multiplikation eine Gruppe, es gibt also unter ihnen insbesondere ein einziges normiertes Element* $\bar{P}$, *den dem Primteiler* p *komplementären normierten Orthogonalteiler, der das neutrale Element der Gruppe ist. Jeder normierte Orthogonalteiler ist allgemeiner auch ein Einheitselement für alle durch ihn teilbaren Elemente. In der Gruppe aller zu* $\bar{P}$ *äquivalenten Orthogonalteiler hat jede Gleichung* $A \cdot X = B$ *oder* $Y \cdot A = B$, *wo* $A \backsim B \backsim \bar{P}$, *je eine einzige Lösung.*

Die normierten Orthogonalteiler von R_{360} sind: 216, 280, 225.

Von nun an sollen hier ausschließlich solche Ringe betrachtet werden, die nur endlichviele wesentlich ver-

schiedene Primteiler, also auch nur endlichviele normierte Orthogonalteiler enthalten. Unter diese Klasse von Ringen fallen im besonderen *alle* Ringe endlichen Grades, dann auch Ringe unendlich hohen Grades, in denen aber jedenfalls mindestens ein Primteiler bis zu einem unendlich großen (symbolischen) Exponenten steigen muß. Für Ringe mit unendlichvielen wesentlich verschiedenen Primteilern wären Summen von unendlichvielen Gliedern zu betrachten, die zunächst keinen Sinn haben und für die erst besonders eine Art Konvergenzuntersuchung — übrigens verschieden von der gewöhnlichen Art einer solchen — zu führen wäre.

Für Ringe $\mathfrak{R}$ mit nur endlichvielen wesentlich verschiedenen Primteilern gilt nun:

Satz 3: *Die Summe aller verschiedenen normierten Orthogonalteiler aus $\mathfrak{R}$ ist gleich dem universalen Einheitselement ε aus $\mathfrak{R}$.*

Z. B. ist in R_{360}: $216 + 280 + 225 = 1$.

Es sei nämlich $(p_1, p_2, \dots p_n)$ ein vollständiges System wesentlich verschiedener Primteiler aus $\mathfrak{R}$; $P_1, P_2, \dots P_n$ seien die ihnen komplementären normierten Orthogonalteiler. Dann ist sicher $\bar{P}_1 + \bar{P}_2 + \cdots + \bar{P}_n = \pi$ regulär; denn durch den Primteiler p_i sind $\bar{P}_1, \bar{P}_2, \dots \bar{P}_{i-1}, \bar{P}_{i+1}, \dots \bar{P}_n$, aber nicht $\bar{P}_i$ und also auch nicht π teilbar. Ferner ist

$$\pi \cdot \pi = \sum_1^n{}_i \bar{P}_i \cdot \bar{P}_i + \sum_1^n{}_i \sum_1^n{}_{k \neq i} \bar{P}_i \cdot \bar{P}_k$$

oder, da nach Satz 2 $\bar{P}_i \cdot \bar{P}_i = \bar{P}_i$, nach Satz 1 $\bar{P}_i \cdot \bar{P}_k = O$ $(i \neq k)$ ist, $\pi \cdot \pi = \pi$. Aus der Gruppeneigenschaft der regulären Elemente folgt schließlich, daß jedes normierte reguläre Element gleich ε ist, womit der Satz bewiesen ist.

Definition 2: Ist A ein beliebiges Element aus $\mathfrak{R}$, $\bar{P}_i$ der dem Primteiler p_i aus $\mathfrak{R}$ komplementäre normierte Orthogonalteiler, so heiße das Produkt $A \cdot \bar{P}_i = A_i$ die Komponente von A in bezug auf den Primteiler p_i*). Diese Bezeichnung rechtfertigt sich durch

Satz 4: *Die Komponente eines Ringelements A in bezug auf den Primteiler p_i ist durch alle und nur solche Potenzen von p_i (allgemeiner durch alle und nur solche Teiler der zu p_i gehörigen Primärteiler) teilbar, durch die A selbst teilbar ist; sie ist dann und nur dann gleich Null, wenn A durch die zu p_i gehörigen Primärteiler teilbar ist.*

*) Hierzu und zum nächstfolgenden vergleiche man die (etwas spezielleren) Verhältnisse bei den g-adischen Zahlen (*Hensel*, Zahlentheorie, S. 86 ff. und 188 ff.).

In der Tat ändert sich ja A in bezug auf seine Teilbarkeit durch p_i gar nicht bei Multiplikation mit dem durch p_i nicht teilbaren Orthogonalteiler P_i; ist aber A durch die zu p_i gehörigen Primärteiler teilbar, so enthält A_i *alle* Primärteiler von $\mathfrak{R}$.

Die Bedeutung der Komponenten liegt in folgendem

Satz 5: *Jedes Element aus $\mathfrak{R}$ ist gleich der Summe seiner Komponenten in bezug auf alle wesentlich verschiedenen Primteiler von $\mathfrak{R}$. Ein Element ist dann und nur dann gleich Null, wenn jede einzelne seiner Komponenten gleich Null ist; zwei Elemente sind dann und nur dann einander gleich, wenn das nämliche von jedem Paar entsprechender Komponenten gilt.*

In der Tat ist: $A = A \cdot \varepsilon = A \cdot \bar{P}_1 + A \cdot \bar{P}_2 + \cdots + A \cdot \bar{P}_n$. Ferner kann ein Element aus $\mathfrak{R}$ nur dann gleich Null sein, wenn es durch jeden Primärteiler teilbar ist, was eben die zwei letzten Behauptungen besagen.

Z. B. ist in R_{360}: $7 = 7 \cdot 225 + 7 \cdot 216 + 7 \cdot 280 = 135 + 72 + 160$; $5 = 5 \cdot 225 + 5 \cdot 216 + 5 \cdot 280 = 45 + 0 + 320$.

Satz 6: *Die Komponente einer Summe bzw. eines Produktes in bezug auf einen Primteiler ist gleich der Summe bzw. dem Produkt der Komponenten der einzelnen Summanden bzw. Faktoren in bezug auf denselben Primteiler.*

Für die Summe ist der Satz selbstverständlich; für das Produkt wird er erhalten durch Multiplikation der Identitäten $A = A_1 + A_2 + \cdots + A_n$, $B = B_1 + B_2 + \cdots + B_n$, wenn man beachtet, daß für $i \neq k$ stets $A_i \cdot B_k = O$ ist, und die letzte Aussage von Satz 5 benutzt.

Definition 3: Ein Ring $\mathfrak{R}$ heiße einfach, wenn alle seine Primteiler untereinander äquivalent sind. Ein einfacher Ring ist natürlich immer zerlegbar.

Offenbar ist die Theorie derartiger Ringe außerordentlich viel einfacher als die der allgemeinen Ringe und in manchen Beziehungen fast ebenso einfach wie die Theorie der Körper; speziell sind die Fragen der Teilbarkeit und Quotientenbildung in einfachen Ringen stets sehr leicht zu entscheiden, da das diesbezügliche Verhalten zweier Elemente zueinander völlig klar ist, sobald man weiß, welches von ihnen die Primteiler von $\mathfrak{R}$ in höherer Potenz enthält.

Man bilde nun zu jedem normierten Orthogonalteiler $\bar{P}_i$ des allge-

meinen Ringes $\mathfrak{R}$ das System $\mathfrak{R}_i$ aller durch $\bar{P}_i$ teilbaren Elemente von $\mathfrak{R}$ oder — was, abgesehen von untereinander gleichen Elementen, das nämliche ist — das System der Komponenten aller Elemente von $\mathfrak{R}$ in bezug auf den Primteiler p_i, dem $\bar{P}_i$ komplementär ist. Jedes solche System $\mathfrak{R}_i$ bildet, wie leicht erkennbar, in bezug auf die im Ring $\mathfrak{R}$ definierten und innerhalb $\mathfrak{R}_i$ stets ausführbaren Operationen der Addition und der Multiplikation einen einfachen Ring, der alle Bedingungen erfüllt, dessen Einheitselement $\bar{P}_i$ ist und dessen Primteiler äquivalent zu $\bar{P}_i \cdot p_i$ sind. Hieraus und aus der Darstellung eines beliebigen Elements von $\mathfrak{R}$ als Summe seiner Komponenten folgt der *fundamentale*

Satz 7: *Jeder beliebige zerlegbare Ring $\mathfrak{R}$, der n wesentlich verschiedene Primteiler der Null enthält, läßt sich stets und nur auf eine einzige Weise in n und nicht weniger einfache Ringe $\mathfrak{R}_1, \mathfrak{R}_2, \ldots \mathfrak{R}_n$ zerlegen derart, daß jeder dieser einfachen Ringe nur Elemente aus $\mathfrak{R}$ enthält, kein Element von $\mathfrak{R}$ (außer der natürlich in jedem $\mathfrak{R}_i$ enthaltenen Null) in zwei verschiedenen der Ringe $\mathfrak{R}_i$ vorkommt, daß ferner das Produkt irgend welcher Elemente aus zwei verschiedenen Ringen $\mathfrak{R}_i$ stets gleich Null ist und schließlich jedes Element aus $\mathfrak{R}$ sich auf eine und nur eine einzige Weise als Summe je eines Elements aus jedem der Ringe $\mathfrak{R}_i$ darstellen läßt.*

So ist z. B. R_{360} zerlegbar in die drei einfachen Ringe:
(0, 72, 144, 216, 288) (Körper), (0, 40, 80, 120, 160, 200, 240, 280, 320),
(0, 45, 90, 135, 180, 225, 270, 315).

Von den Behauptungen dieses Satzes, der also *die Möglichkeit der Zurückführung beliebiger zerlegbarer Ringe auf einfache Ringe* behauptet (die *Art* dieser Zurückführung ergibt sich aus den vorangegangenen Erörterungen), ist noch diejenige zu beweisen, welche besagt, daß diese Zerlegung eines Ringes durch die im Satze ausgesprochenen Eigenschaften *eindeutig* bestimmt ist. Dieser Beweis läßt sich jetzt höchst einfach in vier Schritten führen.

1. Ich zeige zunächst, daß das Einheitselement eines jeden der einfachen Ringe, z. B. das Einheitselement e_1 von $\mathfrak{R}_1$, entweder regulär oder ein Primärteiler oder ein Produkt von Primärteilern ist. In der Tat, ist $e_1 = e_1' \cdot e_1''$, wo e_1' gleichzeitig mit jedem Primteiler den zugehörigen Primärteiler enthält, während e_1'' weder durch einen Primärteiler noch durch einen in e_1' enthaltenen Primteiler teilbar ist, so folgt durch Quadrierung der letzten Beziehung $e_1 \backsim e_1' \cdot e_1''^2$, weil ja e_1 nach Voraussetzung normiert

ist; da aber ein in e_1'' enthaltener Primteiler in $e_1''^2$ in höherer Potenz enthalten sein müßte als in e_1'', ist e_1'' notwendig regulär. Hiermit ist diese erste Behauptung unter alleiniger Benutzung *der Ringeigenschaft der* $\mathfrak{R}_i$ bewiesen.

2. Ich ziehe nun die Eigenschaften der *Orthogonalität der* $\mathfrak{R}_i$ (des Verschwindens der Produkte irgend welcher Elemente aus verschiedenen $\mathfrak{R}_i$) und der *eindeutigen additiven Darstellbarkeit* der Elemente von $\mathfrak{R}$ heran, um zu zeigen, daß jeder der einfachen Ringe, z. B. $\mathfrak{R}_1$, neben seinem Einheitselement e_1 alle Produkte $A \cdot e_1$ enthält, wo A ein beliebiges Element aus $\mathfrak{R}$ bedeutet. Ist nämlich die Darstellung des Elements $A \cdot e_1$ aus $\mathfrak{R}$ als Summe je eines Elements aus jedem einfachen Ring die folgende: $A \cdot e_1 = A_1 + A_2 + \cdots + A_m$, wo m die vorläufig unbekannte Anzahl der $\mathfrak{R}_i$ ist, so gibt die Multiplikation mit e_1: $A \cdot e_1 = A_1 + O + \cdots + O$; hieraus aber folgt wegen der Eindeutigkeit der Darstellung und des Vorkommens der Null in jedem $\mathfrak{R}_i$, daß $A_2 = \cdots = A_m = O$ ist und also $A \cdot e_1$ wirklich in $\mathfrak{R}_1$ vorkommt.

3. Nunmehr ergibt sich unmittelbar aus der *Einfachheit* der $\mathfrak{R}_i$, daß, wenn n die Anzahl der wesentlich verschiedenen Primteiler von $\mathfrak{R}$ bedeutet, jedes der Einheitselemente der $\mathfrak{R}_i$ durch mindestens $n-1$ wesentlich verschiedene Primärteiler teilbar und demnach ein normierter Orthogonalteiler oder Null ist. In der Tat, wäre z. B. e_1, wie es aus der gegenteiligen Annahme wegen 1. folgen würde, durch die wesentlich verschiedenen Primteiler p_i und p_k von $\mathfrak{R}$ nicht teilbar, so wären nach 2. doch $p_i \cdot e_1$ und $p_k \cdot e_1$ Elemente von $\mathfrak{R}_1$ und diese hätten, wie man sich sehr leicht überzeugt, in $\mathfrak{R}_1$ den Charakter zweier wesentlich verschiedener Primteiler.

4. Da also alle Elemente eines jeden Ringes $\mathfrak{R}_i$ durch alle Primteiler bis auf höchstens einen teilbar sind, so muß es, damit z. B. reguläre Elemente additiv dargestellt werden können, mindestens n solche einfache Ringe geben, und zwar genau n, wenn man die trivialen Ringe ausschließt, deren Elemente sämtlich gleich Null sind. Der Beweis für die Eindeutigkeit der Zerlegung ist also völlig erbracht.

Satz 8: *Ist der Ring* $\mathfrak{R}$ *auf die in Satz 7 angegebene Weise in einfache Ringe* $\mathfrak{R}_1, \mathfrak{R}_2, \ldots \mathfrak{R}_n$ *zerlegt, die alle durch* $\bar{P}_1, \bar{P}_2, \ldots \bar{P}_n$ *teilbaren Elemente enthalten, so hat eine Gleichung mit Koeffizienten aus* $\mathfrak{R}$

$$A^{(0)} \cdot X^m + A^{(1)} \cdot X^{m-1} + \cdots + A^{(m-1)} \cdot X + A^{(m)} = O$$

dann und nur dann eine Lösung X *in* $\mathfrak{R}$, *wenn jede der Gleichungen*

$$(i) \qquad A_i^{(0)} \cdot X^m + A_i^{(1)} \cdot X^{m-1} + \cdots + A_i^{(m-1)} \cdot X + A_i^{(m)} = O \qquad (i = 1, 2, \ldots n),$$

wo $A_i^{(k)} = A^{(k)} \cdot \bar{P}_i$ *die Komponente von* $A^{(k)}$ *in bezug auf den Primteiler* p_i, *also ein Element von* $\mathfrak{R}_i$ *bedeutet, in dem einfachen Ring* $\mathfrak{R}_i$ *eine Lösung besitzt. Ist letzteres der Fall und ist* $(X_1, X_2, \ldots X_n)$ *ein System von Lösungen der* n *Gleichungen, so ist das dem Ring* $\mathfrak{R}$ *angehörige Element* $X = X_1 + X_2 + \cdots + X_n$ *eine Lösung der ursprünglichen Gleichung in* $\mathfrak{R}$; *hat im besonderen jede der Gleichungen* (i) *in* $\mathfrak{R}_i$ *endlichviele, und zwar* l_i (> 0) *verschiedene Lösungen, so hat die gegebene Gleichung genau* $l_1 l_2 \cdots l_n$ *verschiedene Lösungen in* $\mathfrak{R}$; *hat auch nur eine der Gleichungen* (i) *unendlichviele verschiedene Lösungen, so hat die gegebene Gleichung, wenn überhaupt eine, dann unendlichviele verschiedene Lösungen.*

In der Tat folgt aus Satz 6, daß die Komponente einer ganzen rationalen Funktion von Elementen aus $\mathfrak{R}$ in bezug auf p_i gleich derjenigen Funktion ist, die aus der ursprünglichen entsteht, wenn für jedes vorkommende Element aus $\mathfrak{R}$ seine Komponente in bezug auf p_i genommen wird. Werden umgekehrt die Gleichungen (i) durch die Elemente X_i der Ringe $\mathfrak{R}_i$ erfüllt, so setze man X_i für X in diesen Gleichungen ein und addiere die so entstandenen n Identitäten im Ringe $\mathfrak{R}$; da alsdann wegen $\bar{P}_i \cdot \bar{P}_k = O$ $(i \neq k)$

$$\begin{aligned} &A_1^{(k)} X_1^{m-k} + A_2^{(k)} X_2^{m-k} + \cdots + A_n^{(k)} X_n^{m-k} \\ &= (A_1^{(k)} + A_2^{(k)} + \cdots + A_n^{(k)}) \cdot (X_1^{m-k} + X_2^{m-k} + \cdots + X_n^{m-k}) \\ &= A^{(k)} \cdot (X_1 + X_2 + \cdots + X_n)^{m-k} \end{aligned}$$

ist, so wird die gegebene Gleichung wirklich durch das Element $X = X_1 + X_2 + \cdots + X_n$ aus $\mathfrak{R}$ erfüllt. Die letzten Behauptungen des Satzes schließlich folgen aus dem Schluß von Satz 5 (S. 37).

Durch Satz 8 ist im besonderen auch die Frage nach der Existenz eines Quotienten zweier Elemente eines allgemeinen Ringes auf die triviale entsprechende Frage für einfache Ringe reduziert.

Besonders einfach gestalten sich diese Ergebnisse, wenn alle Primteiler von $\mathfrak{R}$ nur bis zum Exponenten 1 steigen, wie es z. B. im Ring der Kongruenzklassen für eine beliebige, kein Quadrat enthaltende Zahl als Modul oder in jedem Ring g-adischer Zahlen der Fall ist. Da in Ringen dieser Art ein Element von $\mathfrak{R}$ dann und nur dann durch den Primteiler p_i teilbar ist, wenn seine Komponente in bezug auf p_i gleich Null ist, und da ferner eine Gleichung m-ten Grades bekanntlich in einem Körper höchstens m Wurzeln besitzt, so folgt für diesen Fall:

Satz 9: *Steigen die n wesentlich verschiedenen Primteiler eines Ringes* $\mathfrak{R}$ *sämtlich nur bis zum Exponenten* 1, *so sind die einfachen Ringe* $\mathfrak{R}_i$, *in die sich* $\mathfrak{R}$ *zerlegen läßt, sämtlich (eventuell nichtkommutative) Körper, und eine beliebige Gleichung m-ten Grades in* $\mathfrak{R}$ *hat daher, wenn jeder dieser Körper* $\mathfrak{R}_i$ *unendlichviele verschiedene Elemente enthält, entweder höchstens* m^n *oder unendlichviele verschiedene Lösungen. Insbesondere kann man ein Element A durch ein anderes B in* $\mathfrak{R}$ *dann und nur dann dividieren, wenn für jeden Primteiler* p_i, *für den die zugehörige Komponente von B verschwindet, dasselbe von der zugehörigen Komponente von A gilt; und dann und nur dann ist die Division eindeutig, wenn überhaupt kein Primteiler der letztgenannten Art in* $\mathfrak{R}$ *existiert.*

Schließlich lassen sich die wesentlichsten Resultate dieses Paragraphen auch so formulieren:

Schlußergebnis: *Die Elemente eines beliebigen zerlegbaren Ringes* $\mathfrak{R}$, *der endlichviele und zwar n wesentlich verschiedene Primteiler enthält, lassen sich darstellen als komplexe Zahlen mit n Haupteinheiten* e_i: $A = a_1 e_1 + a_2 e_2 + \cdots + a_n e_n$, *mit denen nach den gewöhnlichen Regeln der Arithmetik zu rechnen ist, nur daß die Multiplikation im allgemeinen nicht kommutativ ist und gemäß den Relationen* $(a_i e_i) \cdot (b_i e_i) = (a_i \cdot b_i) e_i$, $(a_i e_i) \cdot (b_k e_k) = O$ $(i \neq k)$ *ausgeführt wird. Hierbei gehören aber die Koeffizienten der Haupteinheiten keineswegs alle einem und demselben Körper an**), *sondern die Koeffizienten jeder einzelnen Haupteinheit bilden je einen einfachen Ring oder, falls alle Primteiler von* $\mathfrak{R}$ *nur bis zum Exponenten* 1 *steigen, je einen Körper. Umgekehrt genügt jedes derartige System komplexer Zahlen allen in diesem Aufsatz ausgesprochenen Bedingungen und Sätzen.*

Die letzte Behauptung läßt sich leicht rückwärts einsehen; z. B. sind, wenn $\varepsilon_1, \varepsilon_2, \ldots \varepsilon_n$ die Einheitselemente, $p_1, p_2, \ldots p_n$ je irgendwelche Primteiler der n Koeffizientenringe bedeuten, $\varepsilon_1 e_1 + \varepsilon_2 e_2 + \cdots + \varepsilon_n e_n$ das Einheitselement von $\mathfrak{R}$, ferner $\varepsilon_2 e_2 + \varepsilon_3 e_3 + \cdots + \varepsilon_n e_n$, $\varepsilon_1 e_1 + \varepsilon_3 e_3 + \cdots + \varepsilon_n e_n$, $\ldots$ $\varepsilon_1 e_1 + \varepsilon_2 e_2 + \cdots + \varepsilon_{n-1} e_{n-1}$ alle normierten Primärteiler, $p_1 e_1 + \varepsilon_2 e_2 + \cdots + \varepsilon_n e_n$, $\varepsilon_1 e_1 + p_2 e_2 + \cdots + \varepsilon_n e_n$, $\ldots$ $\varepsilon_1 e_1 + \varepsilon_2 e_2 + \cdots + p_n e_n$ ein vollständiges System wesentlich verschiedener normaler Primteiler aus $\mathfrak{R}$ usw..

*) Vgl. *L. E. Dickson*, Transact. of the Amer. Math. Soc., vol. 4 (1903), p. 21 und ferner eine Bemerkung desselben Autors ebenda, vol. 6 (1905), p. 348, die durch die obigen Ausführungen weiter fortgeführt wird.

Verzeichnis der Termini.

	Seite
äquivalent	13
Einheitselement	10
enthalten	13
Exponent, bis zu dem ein Primteiler steigt	23, 25
Grad eines Ringes	14
Gruppe	8
(nichtkommutativer) Körper	11
komplementär (bei Orthogonalteilern)	34
Komponente eines Elements in bezug auf einen Primteiler	36
neutrales Gruppenelement	8/9
normales Element	31
normiertes Element	29
Null, Nullelement	9
Nullteiler	10
Ordnung eines Ringes	14
Orthogonalteiler der Null	34
Paenegruppe	9
Primärteiler der Null	25
Primteiler der Null	15
R_m	13
reguläres Element	10
Ring	9 ff., vgl. 22 u. 35/6
—, einfacher	37
—, endlicher, unendlicher	14
—, kommutativer	11
— der Kongruenzklassen modulo m	13
—, zerlegbarer	18, vgl. 22
teilbar, Teiler (echter —)	13
Teiler der Null	10
unwesentlich verschieden	13
wesentlich verschieden	13

Inhalt.

	Seite
Einleitung	5
§ 1. Die Ringe im allgemeinen	7
§ 2. Die zerlegbaren Ringe, ihre Primteiler und Primärteiler der Null und die multiplikative Zerlegung ihrer Elemente	15
§ 3. Die normierten Primärteiler und die normalen Primteiler	28
§ 4. Die Orthogonalteiler. Die Zerlegung der Ringe	34

Lebenslauf.

Am 17. Februar 1891 wurde ich in München geboren als Sohn des Kaufmanns Sigmund Fraenkel, K. Kommerzienrats in München, und seiner Ehefrau Charlotte, geb. Neuburger; ich bin bayerischer Staatsangehöriger und israelitischen Bekenntnisses. Nach dreijährigem Besuch der Volksschule und neunjährigem Besuch des K. Luitpoldgymnasiums in München erhielt ich im Juli 1909 das Reifezeugnis. Seitdem studierte ich Mathematik, Physik, Nationalökonomie und Philosophie an den Universitäten in München (W.-S. 1909/10 u. S.-S. 1910), Marburg a. d. L. (W.-S. 1910/11 bis W.-S. 1911/12 und S.-S. 1913 bis W.-S. 1913/14) und Berlin (W.-S. 1912/13) sowie an der Technischen Hochschule in München (S.-S. 1912); ich beteiligte mich an Vorlesungen, Seminarübungen und praktisch-physikalischen Arbeiten der Herren: v. Aster, v. Bissing, Burkhardt, Dorn, v. Dyck, Ebert (†), Finsterwalder, Günther, v. d. Leyen, Lindemann, Pringsheim, Röntgen, Schneider, v. Seeliger, Sommerfeld, Voss und Wagner in München, Cohen, v. Dalwigk, Feussner, Hellinger, Hensel, Köppe, Neumann, Richarz, Schenck, F. A. Schulze und Troeltsch in Marburg, Eberstadt, Frobenius, Knoblauch, Knopp, Planck, Schottky, Schur, H. A. Schwarz und v. Wilamowitz-Moellendorf in Berlin.

Das Rigorosum bestand ich am 21. Januar 1914. Gegenwärtig (S.-S. 1914) studiere ich Mathematik und Physik an der Universität und der Technischen Hochschule in Breslau.

All meinen verehrten Lehrern bin ich zu lebhaftem Danke verpflichtet, namentlich aber den Herren Geheimrat Günther in München, Dr. Hellinger in Marburg und Prof. Schur in Berlin, jetzt in Bonn, für ihre wertvolle Förderung und Beratung. Ganz besonders dankbar möchte ich an dieser Stelle bekennen, wie außerordentlich viel in meiner ganzen Entwicklung ich den Herren Geheimrat Hensel in Marburg und Prof. Loewy in Freiburg verdanke, die mir in wissenschaftlichem und persönlichem Verkehr die reichste Anregung, Belehrung und Ermutigung boten und mich stets mit Rat und Tat unterstützten.